FOUNDATIONS OF THE THEORY OF ALGEBRAIC NUMBERS

15836

THE MACMILLAN COMPANY
NEW YORK · BOSTON · CHICAGO · DALLAS
ATLANTA · SAN FRANCISCO

MACMILLAN & CO., LIMITED
LONDON · BOMBAY · CALCUTTA
MELBOURNE

THE MACMILLAN COMPANY
OF CANADA, LIMITED
TORONTO

FOUNDATIONS OF THE THEORY OF ALGEBRAIC NUMBERS

15839

BY

HARRIS HANCOCK, PH.D. (Berlin), DR.Sc. (Paris),

PROFESSOR OF MATHEMATICS IN
THE UNIVERSITY OF CINCINNATI

VOLUME II

THE GENERAL THEORY

PUBLISHED WITH THE AID OF
THE CHARLES PHELPS TAFT MEMORIAL FUND
UNIVERSITY OF CINCINNATI

New York

THE MACMILLAN COMPANY

1932

COPYRIGHT, 1932,
BY THE BOARD OF DIRECTORS
OF THE UNIVERSITY OF CINCINNATI

All rights reserved—no part of this book may be reproduced in any form without permission in writing from the publisher, except by a reviewer who wishes to quote brief passages in connection with a review written for inclusion in magazine or newspaper.

Set up and printed.
Published December, 1932.

512
H19A
Cat

SET UP AND PRINTED BY THE LANCASTER PRESS, INC.
PRINTED IN THE UNITED STATES OF AMERICA

s of this two volumes of this two volumes of this two volume
ated to are dedicated to are dedicated to are dedica
ory of the memory of the memory of the mem

INTRODUCTION

In Volume I of the present work the theory of Dedekind's moduls was systematically developed and extended. The moduls are made fundamental in the derivation and exposition of the Dedekind ideals, through which and the Kronecker forms it is proposed in this second volume to found the General Theory of Algebraic Numbers.

While Hilbert in his monumental work mentioned the moduls only in passing, it is seen that many of the very important theorems and formulas which he used and rightly attributed to Dedekind, have their true origin in the moduls, and are more easily understood if treated from this standpoint. When extended these moduls become the modular systems of Kronecker which in the hands of Hensel pervade the whole theory.

The linear forms with indeterminate coefficients introduced by Kronecker become algebraic numbers, when the indeterminates are replaced by rational numbers; and the "content" of these forms, as Hilbert indicates, are ideals.

The *fundamental* linear form satisfies Kronecker's *fundamental equation* and the left hand side of this equation, considered modulo p, where p is a rational prime integer, may be factored into prime functions that are of the same degrees in the variable as are the respective degrees of the prime ideal factors of p.

This is the basis of the Kronecker theory as treated in Chapter IV, the theory of Dedekind's ideals having occupied the three preceding chapters. Much help was

derived from the works of Hilbert and Hensel in intermingling, intertwining, and juxtaposing the two theories. The works of these two authors were again of great assistance in deriving the divisors of the discriminant and in the treatment of the allied theory of Chapter VI. Of the two methods used, the one is of an arithmetical nature due to Dedekind, the other being more algebraic and due to Hensel, who thereby very essentially extended the Kronecker theory as sketched in the last articles of his *Grundzüge*. And here again the two theories of Dedekind and Kronecker have been put in juxtaposition. Many of the theorems that were proved by Dedekind and Kronecker were proved anew by Hurwitz and are given in Chapter V as a synoptic resumé of what preceded. In Chapter VII is found an exposition of algebraic units from two somewhat different standpoints, the one due to Dirichlet-Dedekind, the other to Minkowski-Hilbert. Chapter VIII contains certain highly interesting and important theorems taken from Minkowski's *Geometry of Numbers*. These theorems greatly simplify the discussions which have to do with algebraic units and with the analytic computation of the number of ideal classes of a given realm. The theory of ideal classes is treated at length in Chapter IX. The article entitled "A Retrospect and a Prospect" which comes at the end of Chapter IX should be read in connection with the present introduction. It serves to describe more in detail the purport of the later theory, particularly for the student who has grasped the full significance of what precedes.

In Chapter VI the regular and the irregular divisors of the discriminant are treated at length. A third class of divisors, the *singular* divisors, have been the cause of great trouble in the development of the theory and have

been treated satisfactorily only by Hensel by means of the expansion of algebraic numbers in series and through the introduction of the so-called p-adic numbers. This subject presented in Chapter XVI is necessary for the complete establishment of the Foundations of the Theory of Algebraic Numbers, and is intimately connected with the expansion of algebraic functions in power series in the neighborhood of branch-points as exemplified particularly in the Riemann Theory. The material that occupies several of the remaining chapters is intended for use in developing further the Kronecker theory, as well as to clarify the theory that occupies Chapter XVI.

Kronecker (*Grundzüge*, p. 5) defines an algebraic number as the root of an irreducible algebraic equation, whose coefficients belong to a realm of rationality (R, R_1, R_2, $\cdots$), where R, R_1, R_2, $\cdots$ are *any* quantities; and he states (*Grundzüge*, pp. 47, 64, 81) that the Dedekind ideal, where $R = 1$, is the starting point of his general theory. With this in view he wished to bring into play functions of many variables, modular systems, etc. In 1859 Dirichlet wrote that "Kronecker had developed completely and with great simplicity" the theory of the most general complex (algebraic) numbers in connection with the theory of reducible forms. What Kronecker did was to initiate this subject. It remains yet to be developed.

Chapter X has to do with Order-Moduls, which are introductory to the Composite Forms that are considered in Chapter XI.

It was proved in Volume I, Chapters III and IV of the present work, that an algebraic realm, whose elements R, R_1, R_2, $\cdots$ are algebraic functions of algebraic numbers, may be replaced by a realm $\Re(\tau)$, which is generated by the one algebraic number τ. From this point

of view we have a treatment of algebraic numbers which are the roots of irreducible algebraic equations, whose coefficients are quantities of $\Re(\tau)$. This theory due in great measure to Hilbert is the subject-matter of Chapter XII. By working out in detail the simple case of algebraic numbers that are the roots of irreducible quadratic equations whose coefficients are functions of θ, where θ is the root of a quadratic equation with rational numbers as coefficient, it is seen that a vast field of further investigation is opened. Chapters XIII, XIV, and XV all have to do with the Galois theory in the Galois realms of rationality. As sub-realms of the Galois realms, the *reduction realm*, the *inertia realm*, the *branch realm*, etc. are duly emphasized.

Hilbert showed that it is just these realms which are required in the gradual factorization of a prime rational integer p into its prime ideal factors that are also adapted for the algebraic solution of the realm, through which the Galois realm of Kronecker is initially determined; and this puts in a clear light the significance of the theory of those algebraic equations that admit solution through the extraction of roots. Thus the intimate relation between the theory of algebraic numbers and algebra is brought to light in a pleasing and attractive manner. It is seen that the two theories have their common source in the Galois realms. These later chapters, essential for the thorough understanding of the present work, are also necessary for the further extension of the Kronecker theory. If Hilbert's theory, as outlined in Chapter XII, is extended along parallel lines, the Hilbert theory checking with that of Kronecker, the author believes that a very perfect structure may be built upon the firm and rigid foundation which he hopes has been established in

the present treatise. This work would include such theories as the Laws of Reciprocity in the general realms of rationality, the complex multiplication of Elliptic Functions, etc. Such and other material offer a store of rich treasures to reward the able investigator who strives to win them.

As is indicated in Volume I this work is of a heuristic nature and as such it should be complete as far as possible in itself. The theory of the Galois groups and a knowledge of the Galois realms of rationality are indispensable for a correct understanding of Hensel's method of treating the *singular* divisors of the discriminant by means of the p-adic numbers as given in Chapter XVI. And this leads at once to his epoch-making discoveries relative to the arithmetical solution of all algebraic equations as indicated in Professor Hensel's letter which follows. The Galois group theory has been thoroughly worked over by both the French and German schools and a beautiful exposition of it is found in the *Algebra* of the late Professor Heinrich Weber. The Hilbert Theory of Galois realms is given in the *Allgemeine Arithmetik der Zahlenkörper* of the late Professor Paul Bachmann. The publishers of these works, Messrs. Friedrich Vieweg und Sohn and B. G. Teubner, have generously allowed me to reproduce much of this work in Chapters XIII and XV of the present volume. And I herewith acknowledge with many thanks their courtesy as I also do that of Professor J. Sommer, whose excellent book *Vorlesungen über Zahlentheorie* has been of very great assistance particularly in Volume I.

I again desire to tender my great obligations to the ever-courteous and helpful staff (particularly to Mr. F. T. E. Sutphen) of the Macmillan Company.

Again I express my profound thanks to my colleague and friend Professor William T. Semple, to Mrs. Louise Taft Semple, and to the other members of the Charles Phelps Taft Memorial Fund for bearing the entire expense of the publication of this work and for their interest in the Department of Mathametics in the University of Cincinnati. It is my hope that this Department will always merit every confidence that is placed in it.

HARRIS HANCOCK.

CINCINNATI, OHIO,
November, 1932.

TRANSLATION OF A LETTER OF PROFESSOR KURT HENSEL

Marburg-Lahn,
Behringweg 7,
July 5, 1932.

My dear Professor Hancock,

I wish to express my warmest thanks for your letter of June 16 and for your beautiful work *The Foundations of the Theory of Algebraic Numbers*, which indeed already in the first introductory volume has so greatly captivated (*gefesselt*) me.

I am greatly pleased that you wish to make use of my articles found in *Crelle's Journal* in your second volume. Its appearance I anticipate with pleasure. I truly believe that in this manner the simplest and most fruitful approach is to be made to the wonderful realm of algebraic numbers. It is a great joy for me that this belief during the last five years has made such headway in the hands of the younger German mathematicians. With the help of the p-adic numbers and in an extraordinary manner, rich in results, they have put in clearer light and shaped anew the great fields of algebra and the theory of numbers.

I am especially pleased to converse with you over the questions which have so strenuously occupied my attention during the last two years, and which now I have completely finished (*durchgekommen*), namely the complete and unique (*einheitlich*) *arithmetical* solution of all algebraic equations, including numerical equations, of all algebraic curves, of all algebraic surfaces, in general of all equations

$$F(x; x_1, x_2, \cdots, x_r) = A_0(x_1, x_2, \cdots, x_r)x^n + A_1(x_1, x_2, \cdots x_r)x^{n-1} + \cdots + A_n(x_1, x_2, \cdots r_r).$$

And here the widest extensions of the p-adic numbers lead to results that are wonderful in their simplicity, and are everywhere easily applicable in all of these theories, results which the theory of functions has never given.

* * *

(signed) KURT HENSEL.

TABLE OF CONTENTS

CHAPTER I

THEORY OF IDEALS

ARTICLE		PAGE
1.	Divisibility	1
2–3.	Ideals Defined	2
4.	The Ideal $\mathfrak{a}$ Defined through $\mathfrak{a}\mathfrak{o}=\mathfrak{a}$, $\mathfrak{o}$ the Order-Modul	6
5–6.	The G. C. D., L. C. M. Product and Quotient of Ideals Are Ideals	8
7.	Principal Ideals. Associated Numbers	11
8.	Reciprocal Ideals	12
9–10.	Theorems Which Have to Do with Reciprocal Ideals, $\mathfrak{o}$ Playing the Rôle of Unity	13
11.	Norms of Ideals	18

CHAPTER II

INTEGRAL IDEALS

12.	Definition	22
13.	The L. C. D., G. C. D., and Product of Integral Ideals Are Ideals	23
14.	The Primary Theorem. If $\mathfrak{c}>\mathfrak{a}$, then Is $\mathfrak{c}=\mathfrak{a}\mathfrak{b}$, where $\mathfrak{b}$ Is an Ideal. The Equivalent Theorem Is: If $\mathfrak{i}$ Is an Ideal, there is Another Ideal $\mathfrak{i}_1$, Such that $\mathfrak{i}\mathfrak{i}_1$ Is a Principal Ideal. A Lemma Due to Dedekind	24
15.	The Generalized Gaussian Theorem	27
16.	A Second Proof	29
17–18.	Ideals Relatively Prime. Theorems	31
19.	Theorems Regarding Norms	37
20.	Theorems Regarding Division by Ideals	40
21.	Every Ideal Is either a Principal Ideal or the G. C.D. of Two Such Ideals	42

ARTICLE		PAGE
22.	The Norm of a Product of Ideals Is the Product of Their Norms	45
23.	Interesting Theorems	47
24.	If $\alpha > \mathfrak{a}$, then $N(\alpha) = N(\mathfrak{a})X$, where X Is a Homogeneous Form	49

CHAPTER III

PRIME IDEALS

25.	An Ideal Is Divisible only by a Finite Number of Ideals	52
26.	If a Product of Several Factors Is Divisible by a Prime Ideal $\mathfrak{p}$, One of the Factors Is Divisible by $\mathfrak{p}$	53
27.	Every Ideal Is a Product of Prime Ideals and the Factorization Is Unique	54
28.	The Fundamental (Basal) Ideal	56
29.	The Degree f of a Prime Ideal	58
30–1.	Dedekind's Fundamental Theorem: If $\mathfrak{o}p$ Is Divisible by the Square of $\mathfrak{p}$, then the Discriminant D is Divisible by p	60
32.	Theorem in Congruences	64
33–4.	A Complete Set of Incongruent Residues. The Theorem $\varphi(\mathfrak{ab}) = \varphi(\mathfrak{a})\varphi(\mathfrak{b})$	64
35.	$\Sigma\varphi(\mathfrak{d}) = N(\mathfrak{i})$, where $\mathfrak{d}$ Is a Divisor of $\mathfrak{i}$	70
36.	Fermat's Theorem	72
37.	Congruences of the mth Degree in a Realm of the mth Degree	73
38.	Wilson's Theorem	76
39.	The Height of an Algebraic Integer	77
40.	The Period of an Algebraic Integer	79
41.	Numbers of the Height Unity	80
42.	Numbers of Height f	82
43.	Prime Functions (Mod. p)	83
44–5.	Number of Height h	85
46.	Primary Prime Functions	88
47–50.	Number of Such Functions of Degree h	89

DISTRIBUTION OF IDEALS INTO CLASSES

ARTICLE		PAGE
51.	Equivalent Ideals	96
52.	Principal Classes; Reciprocal Classes	97
53–5.	The Number of Classes Is Finite	100
56–7.	Applications	106
58.	Any Ideal Has only a Finite Number of Ideal Divisors	109
59.	A Meaning of the Integer f	110
60.	Another Meaning of the Degree f of a Prime Ideal	112
61.	A Primitive Number Satisfies an Irreducible Equation of fth Degree	114
62–3.	Property of Such Numbers	116
64.	Primitive Numbers with Respect to Powers of a Prime Ideal	118
65.	If p Is the Smallest Rational Integer Divisible by $\mathfrak{p}$, p is Prime	119
66.	The Four Fundamental Theorems of the Dedekind Theory	120

CHAPTER IV

THE KRONECKER THEORY OF FORMS

67.	Definitions	123
68.	The Content of a Form. Theorems	124
69.	Unit Forms	126
70.	The Norm of a Form	128
71.	The Fundamental Form ξ and the Fundamental Equation	130
72.	The Congruence (Mod. $\mathfrak{p}$) of Lowest Degree Satisfied by ξ	132
73.	The Irreducible Function $\Pi(x; u_1, u_2, \cdots, u_n)$ (Mod. $\mathfrak{p}$) of Which ξ Is a Root	135
74.	The Congruence of Least Degree (Mod. $\mathfrak{p}\mathfrak{p}_1$) Which ξ Satisfies	136
75.	Factorization (Mod. p) of the Fundamental Equation	137
76.	The Formula $\Delta(\xi) = U^2D$	139
77.	The Hilbert Elements. The Different and the Divisors of the Discriminant	140

CHAPTER V

THE CONTRIBUTIONS OF HURWITZ

ARTICLE		PAGE
78.	The Generalized Theorem of Gauss. Another Proof of the Primary Theorem	142
79.	Theorems in Ideals. The Fundamental Theorem again Proved	146
80.	Theorem Regarding the Content of the Product of Two Forms	148
81.	Lemma Preparatory to the Proof of the Primary Theorem	149
82.	Proof that the Number of Classes Is Finite	151
83.	Proof of the Primary Theorem	151
84.	Further Consequences	153
85.	Existence Proof of the G. C. D. of Algebraic Numbers	154
86.	Ideal Numbers	156
87.	Expression for an Ideal through Two Principal Ideals	157
88.	Equality of Two Ideals. Equivalent Numbers	158

CHAPTER VI

THE DIVISORS OF THE DISCRIMINANT

I. The Irregular Divisors. Hensel's Work

89.	The Index of an Integer	162
90.	The Discriminant of a Number. Irregular Divisors.	163
91.	Correspondence of the Factorization of a Function (Mod. p) and of p into Its Ideal Factors	164
92.	Factorization of the Fundamental Equation (Mod. p)	165
93.	The Formula $\Delta(\xi) = U^2 D$	168
94.	The Fundamental Form Satisfies (Mod. p) No Congruence of Degree Less than That of the Fixed Realm	169
95.	The Prime Factors of the Index	172
96.	Hensel's Theorem Regarding the Irregular Divisors of the Discriminant of an Integer	176
97.	Another Criterion for the Same Theorem	177
98.	The Degree of the Form ξ	179

ARTICLE PAGE

99. Realms in Which the Discriminant of Every Integer Is Divisible by a Definite Prime. Example..... 181
100. A Second Example..... 184
101. Hensel's Theorem Regarding the Divisors of the Index of a Number..... 188

II. The Regular Divisors. The Fundamental Ideal

102. Every Prime p Which Is Divisible by the Square of a Prime Ideal, Divides D. See also Art. 30..... 194
103. The Inverse of Above Theorem..... 195
104. The Ring-Leader of an Order-Modul..... 202
105. An Interesting Consequence..... 208
106. The Ring-Leader and the Fundamental Ideal..... 210
107. The Ring-Leader and the Different..... 213
108–9. The Fundamental Ideal and the Basal Invariant D. 214

CHAPTER VII

ALGEBRAIC UNITS

I. The Dirichlet-Dedekind Theory

110. Definition of Algebraic Unit..... 219
111–2. All Units May Be Expressed through a Finite Number of Them. Roots of Unity. The Number ν. 219
113. Important Lemma..... 222
114. Limiting Values for an Integer and Its Conjugates.. 223
115–9. Distribution of the Fixed Realm and Its Conjugate Realms, so that Above Integers Fall into Two Groups..... 224
120. Derivation of an Infinite Number of Algebraic Integers, Whose Norms Are Less than a Fixed Quantity. A Unit Having Some of Its Conjugates in One Group, Some in the Other..... 230
121. The Determinant of the Logarithms of ν Units and Their Conjugates..... 233
122. Formation of a Determinant of μth Order Different from Zero. A System of $\nu - 1$ Independent Units 235
123. To Every Unit there Belongs a Definite System of Real Numbers..... 237

ARTICLE		PAGE
124.	Reduced Units	238
125.	The Number m of Such Units Is Finite	239
126.	Property of Such Units	240
127.	Fundamental System of Units. The Regulator of the System	241
128.	A Unit Reduced with Respect to a Fundamental System Has only Zero Exponents	243
129.	Every Unit Reduced with Respect to a Fundamental System Is the mth Root of Unity	244
130.	The Theorem of Art. 111 Proved	244
131–3.	Similar Theorems Derived by Bachmann for Order-Moduls	245
134.	An Interesting Theorem in Determinants Due to Minkowski	252
	II. The Hilbert-Minkowski Exposition	
135.	Lemmas Due to Minkowski	255
136.	Theorems Relative to the Absolute Value of the Discriminant	256
137.	Theorem: $N(\alpha) \leqq N(\mathfrak{a}) \lvert \sqrt{D} \rvert$	259
138.	Hilbert's Statement of the Dirichlet (Art. 111) Theorem	260
139.	An Important Lemma	262
140.	Another Derivation of the Determinant of Art. 122. Reduced Units	264
141.	The Dirichlet Theorem Proved	267
142.	The Fundamental Units	269
143.	Theorem Regarding Systems of Independent Units	269
	CHAPTER VIII	
	EXTRACTS FROM MINKOWSKI'S GEOMETRY OF NUMBERS	
144.	Definitions. Distance. Neighborhood. Boundary. Cell. Volume	271
145.	The Computation of the Volume	275
146.	The Functions $S(a, b)$ and $E(a, b)$	279
147.	Example 1. Proof of Fundamental Theorem (Vol. I, Arts. 26 ff.) in Linear Forms	284

ARTICLE PAGE

148. Example 2. The Arithmetical Mean of a System of Linear Functions 285
149. Application to Algebraic Realms 288

CHAPTER IX

THE NUMBER OF IDEAL-CLASSES IN A FIXED REALM

150. Synopsis of Preceding Theory 293
151. Reduced Numbers 296
152. Statement of the Problem 297
153. Computation of the Volume V 301
154. A Digression into the Dirichlet Series. The Function $F(t)$ 304

Applications. The Determination of the Number of Ideal-Classes of a Fixed Realm

155. The Class-Number 313
156. An Infinite Product Expressed through a Zeta-Function 315
157. Landau's Expression for the Class-Number 317
158. Two Important Theorems 321
159. A System of Fundamental Classes 323
160. A Retrospect and a Prospect. Suggestions for Further Developments of the Theory 328

CHAPTER X

THE ORDER-MODULS

161. Definitions 334
162. Ideals of an Order-Modul 335
163. The Ring-Leader Introduced 336
164. The G. C. D., L. C. M., and Product of These Ideals. 337
165. Correspondence of Ideals $\mathfrak{i}$ in $\mathfrak{o}_1$ and in $\mathfrak{o}$. Realm-Ideals 338
166. The Equality $\mathfrak{o}\mathfrak{i}=\mathfrak{j}$ 341
167. Correlation of $\mathfrak{o}$ and $\mathfrak{o}_1$ 342
168. The Primary Theorem 343

ARTICLE PAGE

169. Equivalence of Ideals of an Order-Modul. Classes of Ideals 343
170–3. The Number of Ideal Classes 346

CHAPTER XI

COMPOSITE (FACTORABLE) FORMS

174. Definitions. Discriminant of a Form 354
175. Composite Forms 356
176. Discriminant of a Composite Form and the Fundamental Invariant 357
177. Corresponding to Every Ideal there Is a Unit-Form Whose Discriminant Is the Fundamental Invariant 361
178. Integers Expressed through Unit Forms. The Norms 362
179. Equivalent Forms 364
180. Correspondence between the Composition of Ideal Classes and the Composition of Classes of Forms. 368
181. Forms with Discriminants *Not* Equal to the Fundamental Invariant 371
182. Theorems for Ideals of Order-Moduls Analogous to Those of Realm Ideals 372
183. Still Other Composite Forms. Discriminant of a Class of Moduls 375

CHAPTER XII

RELATIVE REALMS. SUB–REALMS. SUPER–REALMS

184. Definitions 379
185. Properties of the Relative Different and of the Relative Discriminant 383
186. Relation among the Discriminants 384
187. Relation among the Differents 387
188. Discussion of the Laws of Reciprocity 388
189. Fundamental Concepts and Definitions. The Relative Quadratic Realm 390

ARTICLE		PAGE
190.	Basis of the Relative Realm, when the Number of Classes h Is Equal to Unity	392
191.	When the Number h Is Greater than Unity	395
192.	Ideals of the Relative Realm	396
193.	The Relative Different and the Relative Discriminant	398
194.	Theorems Regarding the Divisors of the Relative Discriminant	398
195.	The Prime Ideals of the Relative Realm	400
196.	Criterion as to Whether Prime Ideals in Sub-Realms Are Factorable in the Super-Realms	402
197–8.	The Relative Discriminant, when h is an Odd Integer	408
199–200.	Simple Cases of Hilbert's Quadratic Law of Reciprocity	411
201.	Hilbert's Primary Prime Ideals	414
202.	Examples for the Introduction of the Notion of Class-Realms	420
203.	When the Stock-Realm Is Imaginary	427
204.	When the Stock-Realm Is Real	430
205.	Realms with Odd Class-Number	431
206–7.	Examples	433
208.	Remark Regarding Relative Realms of Higher Degrees	439

CHAPTER XIII

THE GALOIS THEORY. SUBSTITUTIONS. PERMUTATIONS

209.	Primitive and Imprimitive Realms	441
210.	Normal Realms. The Galois Resolvent. The Norm of a Realm Is a Normal Realm	444
211.	The Substitutions of a Normal Realm	447
212.	Composition of Substitutions. Group of Substitutions	450
213.	Permutation Groups. Cyclic Permutations. Abelian Groups	452
214.	The Galois Groups. Isomorphism. Affect	455
215.	Transitive and Intransitive Groups. Systems of Intransitivity	462

ARTICLE PAGE

216. Primitive and Imprimitive Groups. Primitive Realms Have Primitive Groups 463
217. Application of Permutation Groups to Equations. Cauchy's Method. Effect of Permutation Groups upon Functions of Independent Variables. Functions *Belonging* to a Group. The Symmetric Group 469
218. Transpositions. Cycles. Cyclic Permutation 474
219. Permutations of the First and Second Kinds. The Alternating Group 477
220. Divisors of Groups; Sub-Groups and Conjugate Groups. Theorems of Lagrange and of Cauchy .. 488
221. Reduction of the Galois Resolvent. Normal Divisors of a Group. The Lagrange Theorem. The Adjunction of Normal Divisors of a Group. The Intersection of Groups 495
222. The Groups of the Resolvents. The Resolvents ... 501
223. Reduction of the Galois Group through Adjunction of Arbitrary Irrationalities 504
224. Remarks Regarding the Divisors of Groups 507
225. Imprimitive Groups 508
226. Abelian Equations 515
227. Reduction of Abelian Equations to Cyclic Equations. 521

CHAPTER XIV

RELATIONS OF A REALM TO ITS DIVISORS

528
228. Relative Norms 531
229. Primitive Roots of the Prime Ideals 533
230. Relative Discriminants 539
231. Prime Ideals in Relative Normal Realms. Relative Abelian and Relative Cyclic Realms 544
232. Ideals in the Divisors of the Realm $\mathfrak{R}$ 548
233. The Divisor Realms Which Belong to a Prime Ideal. The Separation Realm. The Inertia Realm 551
234. The Branch-Group 556
235. The Higher Branch Realms 558
236. Factorization of the Fundamental Ideal .....

CHAPTER XV

THE GALOIS REALMS OF RATIONALITY

ARTICLE		PAGE
237.	The Galois Equations; Abelian Equations; Cyclic Equations. The Substitutions of the Realm Form a Group. Relative Realms	561
238.	A Direct Establishment of a Theory of Ideals for Galois Realms by Hilbert	566
239.	Foundation of an Ideal Theory for Any Algebraic Realm upon That of Its Associated Galois Realm.	569
240.	The Different of the Galois Realm $\mathfrak{R}$ Is an Invariantive Ideal and Its Discriminant Is a Power of the Different	571
241.	The Arithmetical and Algebraic Relations among the Galois Realm and the Sub-Realms, the Group and the Sub-Groups. The Separation Realm; The Inertia Realm; Their Associated Groups	573
242.	Relations among These Respective Groups. Distribution of a Prime Integer p into Its Prime Ideal Factors	575
243.	The Factorization of p in the Sub-Realms of $\mathfrak{R}$	580
244.	Correlation of the Ideal Factors of a Rational Prime Integer in a Realm and Its Sub-Realm	582
245.	Application of the Above to the Separation Realm	592
246.	The Same for the Inertia Realm. The Branch-Group and the Branch-Realm	595
247.	The One-Stroked Branch-Realm and Associated Group	602
248.	The Two-Stroked, etc., Branch-Realms and Groups. Important Consequences That Have to Do with Algebraic Equations	607
249.	The Powers of Prime Ideals or of Rational Primes That Are Factors of the Different or the Discriminant of $\mathfrak{R}$	610
250.	Minkowski's Theorem Regarding the Units of a Galois Realm	615

CHAPTER XVI

DEVELOPMENT OF ALGEBRAIC NUMBERS IN SERIES. THE p-ADIC NUMBERS

ARTICLE		PAGE
251.	Development of Numbers of a Realm $R(\omega)$ with Respect to an Arbitrary High Power $\mathfrak{p}^m$ of a Prime Ideal as Modulus in Power Series (p-adic Numbers). The Development Numbers ρ and π	620
252.	The Foundations of Hensel's Theory of Algebraic Numbers. A Regular p-adic Series. A Branch-Position	627
253.	The Image Realm	631
254.	The Branch-Discriminant. The Branch-Number. Expression through It of the Power of p That Divides the Image Realm	637
255.	The Images of the Conjugates of $\mathfrak{R}(\omega)$ Form a Number of Systems of Conjugate Realms	641
256.	The Highest Power of p Which Divides the Discriminant of $\mathfrak{R}(\omega)$ Is Determined through the Branch-Numbers That Correspond to the Individual Branch-Discriminants	644

INDEX 649

FOUNDATIONS OF THE THEORY OF ALGEBRAIC NUMBERS

CHAPTER I

THEORY OF IDEALS

ART. **1. Divisibility.** A rational or fractional number λ belonging to a finite realm of rationality $\Omega = \Re(\theta)$ is said to be *divisible* [1] by the algebraic number α of the same realm Ω, if there is in Ω an integral algebraic number ξ such that

$$\lambda = \alpha\xi.$$

When Ω is the realm of rational numbers and the discussion lies in the field of *natural* numbers, we note the existence of a *greatest common divisor* of several numbers, and we have the very important theorem that *if the product of several numbers is divisible by a prime integer* p, *at least one of the factors* must be divisible by p. From this fact it follows that every number is resolvable into a product of its prime factors in one and in only one way.

If, however, Ω is an arbitrary algebraic realm of rationality, we meet with a difficulty: If in the definition of *divisibility* we limit the discussion to a definite realm Ω and if we define divisibility here as we have just done for the realm of rational numbers, there is *no* greatest common divisor of several numbers.[2] If, however, we neglect the realm of rationality Ω and permit the discussion to extend to the general realm of all algebraic numbers, there is something which corresponds to the greatest common divisor in the theory of natural numbers. There are then no prime numbers and the theorem regarding the *unique* factorization (or reduction) of a

[1] Vol. I, Art. 89.
[2] Vol. I, Art. 113.

number into its prime factors does not exist. Since we cannot lose sight of the conception of prime number and of the unique reduction of a number into its prime factors, we must in the extended definition of divisibility limit the discussion to a definite realm of rationality and proceed with our definition with this notion in the foreground. To avoid the difficulty which we have just noted, the conception of divisibility [1] may be extended as follows:

If λ and $\alpha, \beta, \gamma, \cdots$ are arbitrary numbers of the algebraic realm of rationality Ω, then λ is said to be divisible by the complex of numbers $\alpha, \beta, \gamma, \cdots$, if there exist in Ω numbers $\xi, \eta, \zeta, \cdots$, such that (1) they are integral; and

$$\lambda = \alpha\xi + \beta\eta + \gamma\zeta + \cdots. \tag{2}$$

For the case that Ω is the realm of rational numbers such an extension of the conception of divisibility is superfluous,[2] for the rational number λ is divisible by the complex of rational numbers $\alpha, \beta, \gamma, \cdots$, when and only when there is a rational integer w such that $\lambda = \bar{d}w$, where $\bar{d}$ is the greatest common divisor of $\alpha, \beta, \gamma, \cdots$.

In this case, where Ω is the realm of natural numbers, the divisibility through a complex of numbers may be at once replaced by the divisibility through *one* number; and that is, the theory of linear forms in several indeterminates reverts into the theory of linear forms in one indeterminate. However, this is not true for the more general algebraic realms.

ART. **2. Ideal.** All algebraic integers of a realm Ω of the nth degree form a finite modul, which we denoted [3] by $\mathfrak{o}$. If the n algebraic integers $\omega_1, \omega_2, \cdots, \omega_n$

[1] See also Vol. I, Arts. 113 and 206.
[2] Vol. I, Art. 113.
[3] Vol. I, Art. 168.

form a basis of the modul $\mathfrak{o}$, this basis has the property that the linear form

$$\omega_1 x_1 + \omega_2 x_2 + \cdots + \omega_n x_n,$$

for integral rational values of the x's, expresses only *algebraic* integers of the realm Ω. Reciprocally, every algebraic integer of the realm Ω may be expressed through the form

$$\omega_1 x_1 + \omega_2 x_2 + \cdots + \omega_n x_n,$$

where $x_1, x_2, \cdots, x_n$ are rational integers. This modul $\mathfrak{o}$ of the nth degree, which includes all the algebraic integers of this realm, is a "ring-modul."[1] It satisfies, as we have already seen,[2] the two equations

$$\mathfrak{o} = \frac{\mathfrak{o}}{\mathfrak{o}} = \mathfrak{o} \qquad \text{and} \qquad \mathfrak{o}\mathfrak{o} = \mathfrak{o}.$$

We shall designate such an order-modul as the *principal* order-modul of the realm Ω.

Suppose next that $\alpha, \beta, \gamma, \cdots$ are arbitrary numbers of the realm Ω. Then all numbers λ which have the property of being divisible by the complex of numbers $\alpha, \beta, \gamma, \cdots$, and which accordingly may be expressed in the linear form

$$\alpha\xi + \beta\eta + \gamma\zeta + \cdots,$$

where $\xi, \eta, \zeta, \cdots$ are algebraic integers in Ω, constitute a finite modul of the nth order.

In Art. 115, Vol. I, the following definition of a modul was given: A modul is a system of numbers such that the difference of any two numbers of the system is again a number of the system. If then λ and λ' are two numbers that are divisible by the complex $\alpha, \beta, \gamma, \cdots$ and which therefore may be written in the form

$$\lambda = \alpha\xi + \beta\eta + \gamma\zeta + \cdots,$$
$$\lambda' = \alpha\xi' + \beta\eta' + \gamma\zeta' + \cdots,$$

[1] See Hilbert, *Bericht*, p. 237. Such a modul we called in Vol. I, Art. 169, an order- or ring-modul.

[2] Vol. I, Art. 133.

it is clear that

$$\lambda-\lambda'=\alpha(\xi-\xi')+\beta(\eta-\eta')+\gamma(\zeta-\zeta')+\cdots.$$

Since $\xi-\xi'$, $\eta-\eta'$, $\zeta-\zeta'$, $\cdots$ are all algebraic integers, $\lambda-\lambda'$ is divisible by the complex α, β, γ, $\cdots$. Further, since ξ, η, ζ, $\cdots$ are algebraic integers in Ω, they may be expressed in the form

$$\xi=\omega_1x_1+\omega_2x_2+\cdots+\omega_nx_n,$$
$$\eta=\omega_1y_1+\omega_2y_2+\cdots+\omega_ny_n,$$
$$\zeta=\omega_1z_1+\omega_2z_2+\cdots+\omega_nz_n,$$

where $x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_n, z_1, z_2, \cdots, z_n$ are all rational integers. It follows that

$$\lambda=\alpha\omega_1x_1+\alpha\omega_2x_2+\cdots+\alpha\omega_nx_n+\beta\omega_1y_1+\beta\omega_2y_2+\cdots,$$

and consequently the collectivity of numbers λ, which are divisible by the complex α, β, γ, $\cdots$, is the same as the collectivity of the values of a linear form consisting of a number of integral rational indeterminates [1] $x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_n, z_1, z_2, \cdots, z_n$ and with coefficients $\alpha\omega_1, \alpha\omega_2, \cdots, \beta\omega_1, \beta\omega_2, \cdots$, that belong to the realm Ω. The totality of the λ's forms therefore a finite modul in the realm Ω, since the number of numbers $\alpha\omega_1, \alpha\omega_2, \cdots, \alpha\omega_n, \beta\omega_1, \cdots$, is finite and these numbers all belong to the realm Ω. The order [2] of a modul, however, in a realm of the nth degree, is at most equal to n. On the other hand, this order is at least n, since the numbers $\alpha\omega_1, \alpha\omega_2, \cdots, \alpha\omega_n$ are divisible by this modul, and these quantities are linearly independent.[3]

Such a modul which consists of all algebraic numbers λ of the realm Ω, that may be expressed in the form

$$\alpha\xi+\beta\eta+\gamma\zeta+\cdots,$$

where the coefficients α, β, γ, $\cdots$ are integral or fractional

[1] We shall see eventually that this notion leads to the Kronecker Theory of Forms given in Chapt. IV.

[2] Vol. I, Art. 168.

[3] Vol. I, Art. 147.

algebraic numbers of the realm Ω, and where the indeterminates $\xi, \eta, \zeta, \cdots$ are all algebraic integers of the realm Ω, is called an *ideal*, and is denoted by $(\alpha, \beta, \gamma, \cdots)$. Accordingly, *an ideal is a modul of the nth order in a realm of the nth degree, formed by the collectivity of values of a linear form*

$$\alpha\xi+\beta\eta+\gamma\zeta+\cdots,$$

in which $\alpha, \beta, \gamma, \cdots$ *are integral or fractional algebraic numbers of a realm* Ω *of the nth degree, and where the indeterminates* $\xi, \eta, \zeta, \cdots$ *take all the algebraic integral values of* Ω. Every number that belongs to this ideal is said to be *divisible* by the ideal, the analogous terminology of the modul theory [1] being adopted. The ideal $(\alpha, \beta, \gamma, \cdots)$ consists of the collectivity of numbers that may be expressed in the linear form

$$\alpha\xi+\beta\eta+\gamma\zeta+\cdots,$$

where $\xi, \eta, \zeta, \cdots$ are algebraic integers of Ω; and the modul $[\alpha, \beta, \gamma, \cdots]$ consists of the totality of numbers which may be expressed in the linear form

$$\alpha x+\beta y+\gamma z+\cdots$$

for *rational integral values* of $x, y, z, \cdots$. To avoid confusion, the square brackets [ ] are used to indicate a modul.

ART. 3. Let $\mathfrak{a}$ be an ideal, λ a number divisible by $\mathfrak{a}$, and let ω be an arbitrary number divisible by $\mathfrak{o}$, that is, an arbitrary algebraic *integer* in Ω. If $\mathfrak{a}=(\alpha, \beta, \gamma, \cdots)$, then is

$$\lambda=\alpha\xi+\beta\eta+\gamma\zeta+\cdots,$$

where $\xi, \eta, \zeta, \cdots$ are algebraic integers in the realm Ω. It is evident that

$$\lambda\omega=\alpha\xi\omega+\beta\eta\omega+\gamma\zeta\omega+\cdots=\alpha\xi'+\beta\eta'+\gamma\zeta'+\cdots,$$

where $\xi', \eta', \zeta', \cdots$ are algebraic integers of the realm Ω;

[1] Vol. I, Art. 114.

and consequently $\lambda\omega$ is divisible by $\mathfrak{a}$. If then λ is a number divisible by the ideal $\mathfrak{a}$, and ω is an algebraic integer of Ω, it is seen that $\lambda\omega$ is divisible by $\mathfrak{a}$. In a similar manner, the sum of such products,

$$\sum(\lambda\omega) = \lambda_1\omega^{(1)} + \lambda_2\omega^{(2)} + \cdots + \lambda_k\omega^{(k)},$$

is divisible by $\mathfrak{a}$, where $\lambda_1, \lambda_2, \cdots, \lambda_k$ are arbitrary numbers divisible by the ideal $\mathfrak{a}$; $\omega^{(1)}, \omega^{(2)}, \cdots, \omega^{(k)}$ being arbitrary algebraic integers of the realm Ω are consequently integers of $\mathfrak{o}$. If then $\mathfrak{a}$ is an ideal, it follows that

$$\mathfrak{a}\mathfrak{o} > \mathfrak{a}.$$

Reciprocally, it is asserted: If $\mathfrak{a}\mathfrak{o} > \mathfrak{a}$, then $\mathfrak{a}$ is an ideal, provided of course that $\mathfrak{a}$ is a modul of the realm Ω of the nth degree. For, if $\mathfrak{a}$ is a modul in the realm Ω, then $\mathfrak{a}$ has a basis which consists of at most n elements, say, $\alpha, \beta, \gamma, \cdots$. If ξ is an arbitrary algebraic integer of the realm Ω, it is divisible by $\mathfrak{o}$, and since α is divisible by $\mathfrak{a}$, it follows that $\alpha\xi$ is divisible by $\mathfrak{a}\mathfrak{o}$. Since by hypothesis $\mathfrak{a}\mathfrak{o}$ is divisible by $\mathfrak{a}$, we see that $\alpha\xi$ is divisible by $\mathfrak{a}$. Further, if η is an arbitrary integer in Ω, then η is divisible by $\mathfrak{o}$. Since β is divisible by $\mathfrak{a}$, we have $\beta\eta$ divisible by $\mathfrak{a}\mathfrak{o}$, and consequently also by $\mathfrak{a}$. It is thus shown that all algebraic numbers of the form

$$\alpha\xi + \beta\eta + \cdots,$$

where $\xi, \eta, \cdots$ are all possible algebraic integers of Ω, are divisible by $\mathfrak{a}$. Since $\alpha, \beta, \gamma, \cdots$ are numbers belonging to the realm Ω, this is the definition of the ideal $\mathfrak{a}$ as given in Art. 2. If $\mathfrak{a}\mathfrak{o} > \mathfrak{a}$, and if $\mathfrak{a}$ is a modul of the realm Ω, then $\mathfrak{a}$ is an ideal. The property $\mathfrak{a}\mathfrak{o} > \mathfrak{a}$ is *characteristic* of an ideal. In the sequel it will be taken as the *definition of an ideal.*

ART. **4.** If $\mathfrak{a}$ is an ideal, then in virtue of this new definition, it may be proved that not only is $\mathfrak{a}\mathfrak{o} > \mathfrak{a}$, but

that $\mathfrak{a}\mathfrak{o}=\mathfrak{a}$. For, since $\mathfrak{a}>\mathfrak{a}$ and $[1]>\mathfrak{o}$, it follows that $\mathfrak{a}[1]>\mathfrak{a}\mathfrak{o}$ or $\mathfrak{a}>\mathfrak{a}\mathfrak{o}$. On the other hand, since $\mathfrak{a}$ is an ideal, we also have $\mathfrak{a}\mathfrak{o}>\mathfrak{a}$, and hence it follows that

$$\mathfrak{a}\mathfrak{o}=\mathfrak{a}.$$

If $\mathfrak{a}$ is an ideal, then also is $\frac{\mathfrak{a}}{\mathfrak{o}}=\mathfrak{a}$; for, since $\mathfrak{a}\mathfrak{o}>\mathfrak{a}$, we have $\mathfrak{a}>\frac{\mathfrak{a}}{\mathfrak{o}}$. On the other hand[1] $\frac{\mathfrak{a}}{\mathfrak{o}}>\frac{\mathfrak{a}}{[1]}$, for $\mathfrak{a}>\mathfrak{a}$ and $[1]>\mathfrak{o}$. We have, therefore,

$$\frac{\mathfrak{a}}{\mathfrak{o}}=\mathfrak{a}.$$

If $\mathfrak{a}$ is an ideal, it may be proved that $\mathfrak{a}^0=\mathfrak{o}$, that is, $\frac{\mathfrak{a}}{\mathfrak{a}}=\mathfrak{o}$. For, since $\mathfrak{a}\mathfrak{o}>\mathfrak{a}$, we have

$$\mathfrak{o}>\frac{\mathfrak{a}}{\mathfrak{a}} \qquad \text{or} \qquad \mathfrak{o}>\mathfrak{a}^0.$$

On the other hand, the order-modul of an ordinary modul of finite order consists only of integral numbers, so that always $\mathfrak{a}^0>\mathfrak{o}$. It follows that[2]

$$\mathfrak{a}^0=\mathfrak{o},$$

and consequently the order-modul of an ideal is the *fundamental order-modul.* This property of an ideal also serves to define it. We may then say that *those finite moduls of the realm* Ω, *whose order-modul is equal to the fundamental* $\mathfrak{o}$ *are ideals.* This is the best (*foundation*) definition of the ideal. The fundamental order-modul is itself an ideal, since $\mathfrak{o}\mathfrak{o}=\mathfrak{o}$. Again observe[3] that the order-modul $\mathfrak{o}$ occupies the same place in the present theory as does unity in the usual theory of natural numbers.

[1] See Vol. I, Art. 132.
[2] Vol. I, Arts. 132, 169.
[3] Vol. I, Art. 133, end.

The order of every ideal $(\alpha, \beta, \gamma, \cdots)$ in the realm Ω of the nth degree is equal to n. For, on the one hand, the order of a modul in a realm of the nth degree $\leqq n$, and on the other hand, the order of an ideal $\geqq n$, because there exists for the ideal a system of n independent quantities, namely,

$$\alpha\omega_1, \alpha\omega_2, \cdots, \alpha\omega_n,$$

where $(\omega_1, \omega_2, \cdots, \omega_n)$ form a fundamental system in Ω, in fact, a basis of all integers of this realm. *Ideals are therefore certain moduls of the nth order in the realm Ω of the nth degree.*

ART. **5.** We shall next prove the following theorems: (1) the greatest common divisor, (2) the least common multiple, (3) the product, (4) the quotient of two ideals are themselves ideals.

Proof. If $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals, it has been shown that

$$\mathfrak{a}\mathfrak{o} = \mathfrak{a} \qquad \text{and} \qquad \mathfrak{b}\mathfrak{o} = \mathfrak{b}.$$

From Vol. I, Art. 121, it follows that

$$(1) \qquad (\mathfrak{a}+\mathfrak{b})\mathfrak{o} = \mathfrak{a}\mathfrak{o}+\mathfrak{b}\mathfrak{o} = \mathfrak{a}+\mathfrak{b}.$$

Consequently, $\mathfrak{a}+\mathfrak{b}$ is an ideal. For, on the one hand, $\mathfrak{a}+\mathfrak{b}$ is a finite modul of the realm Ω, and on the other hand, $(\mathfrak{a}+\mathfrak{b})\mathfrak{o} > \mathfrak{a}+\mathfrak{b}$.

Similarly, as was shown in Vol. I, Art. 124, it follows that

$$(2) \qquad \mathfrak{o}(\mathfrak{a}-\mathfrak{b}) > \mathfrak{o}\mathfrak{a}-\mathfrak{o}\mathfrak{b}.$$

To be able to say that the product of two moduls $\mathfrak{a}\mathfrak{b}$ is an ideal, we need only assume that one of the two moduls is an ideal. If then $\mathfrak{a}$ is an ideal,

$$(3) \qquad \mathfrak{o}(\mathfrak{a}\mathfrak{b}) = (\mathfrak{o}\mathfrak{a})\mathfrak{b} = \mathfrak{a}\mathfrak{b},$$

and $\mathfrak{b}$ must of course be a finite modul.

That the quotient of two finite moduls should be an ideal, it is only necessary to assume that either the numerator or the denominator is an ideal. For example,

if $\frac{\mathfrak{b}}{\mathfrak{a}}$ is a finite modul, and if $\mathfrak{b}$ is an ideal, then $\left(\frac{\mathfrak{b}}{\mathfrak{a}}\right)\mathfrak{o} > \frac{\mathfrak{b}\mathfrak{o}}{\mathfrak{a}}$, and since $\mathfrak{b}\mathfrak{o} = \mathfrak{b}$, it follows that

$$\left(\frac{\mathfrak{b}}{\mathfrak{a}}\right)\mathfrak{o} > \frac{\mathfrak{b}}{\mathfrak{a}}.$$

On the other hand, if $\mathfrak{a}$ is an ideal, then $\mathfrak{a}\frac{\mathfrak{b}}{\mathfrak{a}} > \mathfrak{b}$ and since $\mathfrak{a} = \mathfrak{a}\mathfrak{o}$, we have

$$(4) \qquad \mathfrak{a}\mathfrak{o}\frac{\mathfrak{b}}{\mathfrak{a}} > \mathfrak{b} \qquad \text{or} \qquad \mathfrak{o}\frac{\mathfrak{b}}{\mathfrak{a}} > \frac{\mathfrak{b}}{\mathfrak{a}}.$$

ART. 6. A more detailed proof of the above theorems is as follows:

(1) $\mathfrak{a}+\mathfrak{b}$ consists of the collectivity of numbers $\alpha+\beta$, where α takes all values that are divisible by $\mathfrak{a}$, and β assumes all values that are divisible by $\mathfrak{b}$. Further, let ω be an arbitrary integer in Ω and consequently an arbitrary number that is divisible by $\mathfrak{o}$. It follows, if $\delta = \alpha+\beta$, that

$$\omega\delta = \omega\alpha + \omega\beta.$$

If, further, $\mathfrak{a}$ and $\mathfrak{b}$ are ideals, it is seen that $\omega\alpha$ is divisible by $\mathfrak{a}$, and $\omega\beta$ by $\mathfrak{b}$; and consequently, $\omega\delta$, that is, $\omega\alpha+\omega\beta$ is divisible by $\mathfrak{a}+\mathfrak{b}$. It is thus shown that $\mathfrak{o}(\mathfrak{a}+\mathfrak{b}) > \mathfrak{a}+\mathfrak{b}$ and as $\mathfrak{a}+\mathfrak{b}$ is a finite modul, $\mathfrak{a}+\mathfrak{b}$ is an ideal.

(2) If $\mathfrak{a}$ and $\mathfrak{b}$ are two finite moduls, then the finite modul

$$\mathfrak{m} = \mathfrak{a} - \mathfrak{b}$$

consists of the totality of numbers, which are divisible by both $\mathfrak{a}$ and $\mathfrak{b}$. If, further, ω is an arbitrary algebraic integer in Ω, to which realm the moduls $\mathfrak{a}$ and $\mathfrak{b}$ both belong, and if μ is an arbitrary number divisible by $\mathfrak{m}$, so that $\mu = \alpha - \beta$, where α is divisible by $\mathfrak{a}$, and β by $\mathfrak{b}$, then is

$$\mu\omega = \alpha\omega - \beta\omega.$$

If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals, $\alpha\omega$ is divisible by $\mathfrak{a}$, and $\beta\omega$ is

divisible by $\mathfrak{b}$; and consequently $\mu\omega$ is divisible by $\mathfrak{a}$ and by $\mathfrak{b}$, and therefore also by $\mathfrak{m}$. Since the sum of all such products $\mu\omega$ is divisible by $\mathfrak{m}$, it follows that $\mathfrak{m}\mathfrak{o} > \mathfrak{m}$; and as $\mathfrak{m}$ is a finite modul, it is seen that $\mathfrak{m}$ is an ideal.

(3) If $\mathfrak{a}$ and $\mathfrak{b}$ are two moduls of the realm Ω, the product $\mathfrak{a}\mathfrak{b}$ consists of all quantities $\gamma = \sum(\alpha\beta)$, where α takes all values that are divisible by $\mathfrak{a}$, and β takes all values that are divisible by $\mathfrak{b}$. If further ω is an arbitrary algebraic integer in Ω, and consequently a number divisible by $\mathfrak{o}$, we have

$$\omega\gamma = \sum(\alpha\beta\omega) = (\omega\alpha)\beta + (\omega\alpha')\beta' + \cdots,$$

where $(\omega\alpha) = x\omega\alpha$, x taking all rational integral values, as does x' in $(\omega\alpha') = x'\omega\alpha'$, etc. Assume that $\mathfrak{a}$ is an ideal. It follows then that $\omega\alpha$, $\omega\alpha'$, $\cdots$ are all divisible by $\mathfrak{a}$, and consequently $\omega\alpha\beta$, $\omega\alpha'\beta'$, $\cdots$, and therefore also $\gamma\omega$ are divisible by $\mathfrak{a}\mathfrak{b}$. If then an arbitrary number taken from $\mathfrak{a}\mathfrak{b}$ is multiplied by an arbitrary number of $\mathfrak{o}$, the product is divisible by $\mathfrak{a}\mathfrak{b}$, and consequently also $\mathfrak{a}\mathfrak{b}\mathfrak{o} > \mathfrak{a}\mathfrak{b}$, so that $\mathfrak{a}\mathfrak{b}$ is an ideal.

(4) Let κ be an arbitrary number divisible by $\frac{\mathfrak{b}}{\mathfrak{a}}$, so that $\kappa\mathfrak{a} > \mathfrak{b}$. If then α is an arbitrary number divisible by $\mathfrak{a}$, then $\kappa\alpha$ is equal to some number divisible by $\mathfrak{b}$, say β. If further ω is divisible by $\mathfrak{o}$, then $\kappa\alpha\omega = \beta\omega$. If we assume that $\mathfrak{b}$ is an ideal, then $\kappa\omega\alpha = \beta\omega$ is divisible by $\mathfrak{b}$, so that $\kappa\omega\mathfrak{a} > \mathfrak{b}$, and consequently $\kappa\omega > \frac{\mathfrak{b}}{\mathfrak{a}}$. Hence, since the product formed by an arbitrary number of the modul $\frac{\mathfrak{b}}{\mathfrak{a}}$ and an arbitrary integer of $\mathfrak{o}$ is always divisible by $\frac{\mathfrak{b}}{\mathfrak{a}}$, it follows that $\frac{\mathfrak{b}}{\mathfrak{a}}$ is an ideal.

If, on the other hand, we assume that $\mathfrak{a}$ is an ideal, $\mathfrak{b}$ being of course a finite modul, and if κ is divisbile by $\frac{\mathfrak{b}}{\mathfrak{a}}$, then $\mathfrak{a}\kappa > \mathfrak{b}$. But since $\mathfrak{a}\mathfrak{o} = \mathfrak{a}$, we also have

$$\mathfrak{a}\mathfrak{o}\kappa > \mathfrak{b} \qquad \text{or} \qquad \mathfrak{o}\kappa > \frac{\mathfrak{b}}{\mathfrak{a}}.$$

Since κ is any number of $\frac{\mathfrak{b}}{\mathfrak{a}}$, it follows that $\frac{\mathfrak{b}}{\mathfrak{a}}$ is an ideal.

As $\mathfrak{o}$ is itself an ideal, it follows from the theorems just proved, if $\mathfrak{f}$ is an arbitrary finite modul of Ω, that $\mathfrak{f}\mathfrak{o} > \frac{\mathfrak{f}}{\mathfrak{o}}$ and is an ideal, as is $\frac{\mathfrak{o}}{\mathfrak{f}}$.

ART. 7. **Principal Ideal.** If α is an arbitrary number of the realm Ω, then $\mathfrak{o}\alpha$ is always an ideal, for $\mathfrak{o}(\mathfrak{o}\alpha) = \mathfrak{o}^2\alpha > \mathfrak{o}\alpha$. Such an ideal is called a *principal ideal* (Haupt-ideal) and sometimes written (α). The number α is said to *produce* the principal ideal $\mathfrak{o}\alpha$. This principal ideal consists of numbers of the form $\alpha\xi$, where ξ takes all values that are divisible by $\mathfrak{o}$, that is, all integral values of Ω. The principal ideal $\mathfrak{o}\beta$ consists of all numbers of the form $\beta\eta$, where η takes all values divisible by $\mathfrak{o}$, etc. The collectivity of values

$$\alpha\xi + \beta\eta + \gamma\zeta + \cdots,$$

where ξ, η, ζ, $\cdots$ are arbitrary integers in Ω, and consequently divisible by $\mathfrak{o}$, form the ideal $(\alpha, \beta, \gamma, \cdots)$. This ideal is consequently the *greatest common divisor* of the ideals $\alpha\mathfrak{o}$, $\beta\mathfrak{o}$, $\cdots$. It follows that every ideal is either itself a principal ideal or the greatest common divisor of several such ideals.

If Ω is the realm of rational (natural) numbers, then there are only principal ideals, since here $(a_1, a_2, \cdots, a_n) \sim (d)$, where d is the greatest common divisor of $a_1, a_2,$

$\cdots, a_n$. On this account there is no need of the theory of ideals in the treatment of natural numbers.[1]

It will be seen later (Art. 21) that if Ω is an arbitrary realm of finite degree, every ideal that is not a principal ideal may be expressed as the greatest common divisor of *two* principal ideals.

If ϵ is an algebraic unit, that is, if ϵ and $1/\epsilon$ are algebraic integers, then the principal ideal which is produced by this algebraic number is

$$\mathfrak{o}\epsilon = \mathfrak{o}.$$

For, $\mathfrak{o}\epsilon$ consists of the collectivity of numbers $\omega\epsilon$, where ω takes all values divisible by $\mathfrak{o}$, and consequently

$$\mathfrak{o}\epsilon > \mathfrak{o}. \tag{1}$$

On the other hand, since $[1] > \mathfrak{o}\epsilon$, it follows that $\mathfrak{o}[1] > \mathfrak{o}\mathfrak{o}\epsilon$, or

$$\mathfrak{o} > \mathfrak{o}\epsilon. \tag{2}$$

From (1) and (2) it is seen that

$$\mathfrak{o} = \mathfrak{o}\epsilon.$$

If α is an arbitrary number of the realm Ω, it follows from what we have just seen that

$$\mathfrak{o}\epsilon\alpha = \mathfrak{o}\alpha = (\alpha).$$

Two numbers such as α and $\epsilon\alpha$, which differ only by a multiplicative unit are called *associated* numbers.[2] We have the theorem:

Associated numbers produce the same principal ideals. For a number that is divisible by $\mathfrak{o}\alpha$ is also divisible by $\mathfrak{o}\epsilon\alpha$ and vice versa.

ART. **8. Reciprocal Ideals.** THEOREM. *If* $\mathfrak{a}$ *is an ideal different from zero in the realm* Ω, *there is always one and only one ideal* $\mathfrak{b}$ *in* Ω, *such that* $\mathfrak{a}\mathfrak{b} = \mathfrak{o}$.

[1] Vol. I, Art. 113.
[2] Vol. I, Art. 91.

We have already seen [1] that there is always a modul $\mathfrak{f}$ in Ω such that $\mathfrak{af} = u_1$, where u_1 is a unit-modul, and that is, a modul which contains only algebraic integers of Ω, including unity.

It follows that

$$\mathfrak{a}o\mathfrak{f} = ou_1.$$

If then we write $o\mathfrak{f} = \mathfrak{b}$, then $\mathfrak{b}$ is an ideal in Ω, and we have

$$\mathfrak{ab} = ou_1.$$

Since u_1 is a unit-modul, $u_1 > o$, and consequently $ou_1 > oo > o$. On the other hand, 1 is divisible by u_1, and consequently $o \cdot 1$ or $o > ou_1$. It follows that $ou_1 = o$, and also that $\mathfrak{ab} = o$.

To prove the second part of the theorem, namely, that there is *only* one ideal $\mathfrak{b}$, such that $\mathfrak{ab} = o$, assume that there is a second ideal $\mathfrak{c}$, where

$$\mathfrak{ac} = o.$$

Since $\mathfrak{c}$ is an ideal, it would follow that $co = c$ and that

$$\mathfrak{abc} = (\mathfrak{ab})c = oc = c.$$

Similarly, it is seen that

$$\mathfrak{abc} = (\mathfrak{ac})\mathfrak{b} = o\mathfrak{b} = \mathfrak{b};$$

and consequently

$$\mathfrak{b} = c.$$

This ideal $\mathfrak{b}$ which is uniquely determined through the relation $\mathfrak{ab} = o$, is denoted by $\mathfrak{a}^{-1}$. Thus it is seen that $\mathfrak{aa}^{-1} = o$. It is evident that $\mathfrak{a}^{-1} \neq 0$, since $o \neq 0$. If $\mathfrak{b} = \mathfrak{a}^{-1}$, then $\mathfrak{b}^{-1} = \mathfrak{a}$, and consequently $(\mathfrak{a}^{-1})^{-1} = \mathfrak{a}$. For this reason we may call the two ideals $\mathfrak{a}$ and $\mathfrak{a}^{-1}$ *reciprocal* ideals.

ART. 9. The theorem of the preceding article may be generalized as follows: If $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals in Ω, there

[1] Vol. I, Art. 163.

is in Ω one and only one ideal $\mathfrak{f}$, such that

$$\mathfrak{a}\mathfrak{f} = \mathfrak{b},$$

and $\mathfrak{f} = \mathfrak{b}\mathfrak{a}^{-1}$ is this ideal.

We have also the important result

$$\frac{\mathfrak{b}}{\mathfrak{a}} = \mathfrak{b}\mathfrak{a}^{-1}.$$

For, suppose there is an ideal $\mathfrak{f}$ such that $\mathfrak{a}\mathfrak{f} = \mathfrak{b}$. We then have

$$\mathfrak{a}^{-1}\mathfrak{a}\mathfrak{f} = \mathfrak{b}\mathfrak{a}^{-1}.$$

And, since $\mathfrak{a}^{-1}\mathfrak{a}\mathfrak{f} = \mathfrak{o}\mathfrak{f}$, and since furthermore $\mathfrak{f}$ is an ideal, so that $\mathfrak{o}\mathfrak{f} = \mathfrak{f}$, it is seen that

$$\mathfrak{f} = \mathfrak{b}\mathfrak{a}^{-1}.$$

That this ideal $\mathfrak{f}$ satisfies the condition $\mathfrak{a}\mathfrak{f} = \mathfrak{b}$, is seen at once, since

$$\mathfrak{a}\mathfrak{f} = \mathfrak{a}\mathfrak{b}\mathfrak{a}^{-1} = \mathfrak{o}\mathfrak{b} = \mathfrak{b}.$$

It is further evident that $\mathfrak{f} = \mathfrak{b}\mathfrak{a}^{-1}$ is the only ideal in Ω which satisfies the condition $\mathfrak{a}\mathfrak{f} = \mathfrak{b}$.

If, however, $\mathfrak{f} = \mathfrak{b}\mathfrak{a}^{-1}$, then $\mathfrak{a}\mathfrak{f} = \mathfrak{b}$ and consequently $\mathfrak{a}\mathfrak{f} > \mathfrak{b}$. Hence,

$$\mathfrak{f}\mathfrak{a}\mathfrak{b}\mathfrak{a}^{-1} > \frac{\mathfrak{b}}{\mathfrak{a}}. \tag{1}$$

On the other hand, $\frac{\mathfrak{b}}{\mathfrak{a}}\mathfrak{a} > \mathfrak{b}$, and consequently $\frac{\mathfrak{b}}{\mathfrak{a}}\mathfrak{a}\mathfrak{a}^{-1}$ or $\frac{\mathfrak{b}}{\mathfrak{a}}\mathfrak{o} > \mathfrak{b}\mathfrak{a}^{-1}$. And since $\frac{\mathfrak{b}}{\mathfrak{a}}$ is an ideal, being the quotient of two ideals, it follows that

$$\frac{\mathfrak{b}}{\mathfrak{a}} > \mathfrak{b}\mathfrak{a}^{-1}. \tag{2}$$

From (1) and (2) we obtain

$$\frac{\mathfrak{b}}{\mathfrak{a}} = \mathfrak{b}\mathfrak{a}^{-1}.$$

In the case of a principal ideal, say $\mathfrak{o}\alpha$, where α is an arbitrary number of the realm Ω, it may be proved that

$$(\mathfrak{o}\alpha)^{-1} = \mathfrak{o}\alpha^{-1}.$$

For

$$\mathfrak{o}\alpha\mathfrak{o}\alpha^{-1} = \mathfrak{o}\alpha\alpha^{-1} = \mathfrak{o};$$

and from this it follows that

$$\mathfrak{o}\alpha^{-1} = (\mathfrak{o}\alpha)^{-1}.$$

If $\alpha = 1$, it follows from the last result that $\mathfrak{o}^{-1} = \mathfrak{o}$. It is also seen that if $\mathfrak{a}$ is an arbitrary ideal in Ω; and if we write $\mathfrak{b} = \mathfrak{o}$, then is $\mathfrak{o}\mathfrak{a}^{-1} = \frac{\mathfrak{o}}{\mathfrak{a}}$. And since $\mathfrak{a}^{-1}$ is an ideal,

$$\mathfrak{a}^{-1} = \frac{\mathfrak{o}}{\mathfrak{a}}.$$

From this it is seen again that in this theory $\mathfrak{o}$ plays the rôle of unity.

We further have

$$(\mathfrak{a}\mathfrak{b})^{-1} = \mathfrak{a}^{-1}\mathfrak{b}^{-1}.$$

For, writing

$$(\mathfrak{a}\mathfrak{b})^{-1} = \mathfrak{f},$$

it follows that $\mathfrak{f}$ is uniquely determined through the condition

$$\mathfrak{a}\mathfrak{b}\mathfrak{f} = \mathfrak{o}.$$

Since

$$\mathfrak{a}\mathfrak{b}\mathfrak{a}^{-1}\mathfrak{b}^{-1} = \mathfrak{a}\mathfrak{a}^{-1}\mathfrak{b}\mathfrak{b}^{-1} = \mathfrak{o}\mathfrak{o} = \mathfrak{o},$$

it follows that

$$(\mathfrak{a}\mathfrak{b})^{-1} = \mathfrak{f} = \mathfrak{a}^{-1}\mathfrak{b}^{-1}.$$

From this it follows also that

$$(\mathfrak{a}\mathfrak{b}\mathfrak{c}\cdots)^{-1} = \mathfrak{a}^{-1}(\mathfrak{b}\mathfrak{c}\cdots)^{-1} = \mathfrak{a}^{-1}\mathfrak{b}^{-1}(\mathfrak{c}\cdots)^{-1} = \mathfrak{a}^{-1}\mathfrak{b}^{-1}\mathfrak{c}^{-1}\cdots.$$

Writing

$$\mathfrak{a} = \mathfrak{b} = \mathfrak{c} = \cdots,$$

it follows that

$$(\mathfrak{a}^n)^{-1} = (\mathfrak{a}^{-1})^n.$$

This latter ideal we shall symbolize by $\mathfrak{a}^{-n}$.

It is seen from this that $\mathfrak{a}^{-n}$ may be regarded as either the reciprocal ideal to $\mathfrak{a}^n$, or as the nth power of the ideal

that is reciprocal to $\mathfrak{a}$. From this definition it is clear that the following theorems are true for the *negative* values of the exponents:

$$(\mathfrak{ab})^n = \mathfrak{a}^n\mathfrak{b}^n,$$
$$(\mathfrak{abc}\cdots)^n = \mathfrak{a}^n\mathfrak{b}^n\mathfrak{c}^n\cdots,$$
$$(\mathfrak{a}^n)^s = \mathfrak{a}^{ns},$$
$$\mathfrak{a}^r\mathfrak{a}^s = \mathfrak{a}^{r+s}.$$

That these theorems are true for positive values (including zero) of the exponents, follows from the general modul theory.[1]

ART. **10.** In the theory of ideals many theorems of the general modul theory assume a more complete form, in that equality takes the place of divisibility. This is illustrated in the following theorems:

In the general modul theory[2] we have the theorem $\frac{\mathfrak{b}}{\mathfrak{a}} > \frac{\mathfrak{bc}}{\mathfrak{ac}}$. If, however, $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ are ideals, then

$$\frac{\mathfrak{b}}{\mathfrak{a}} = \frac{\mathfrak{bc}}{\mathfrak{ac}}.$$

For,

$$\frac{\mathfrak{bc}}{\mathfrak{ac}} = \mathfrak{bc}(\mathfrak{ac})^{-1} = \mathfrak{ba}^{-1}\mathfrak{cc}^{-1} = \mathfrak{ba}^{-1}\mathfrak{o} = \mathfrak{ba}^{-1} = \frac{\mathfrak{b}}{\mathfrak{a}}.$$

In the general modul theory

$$\frac{\mathfrak{b}}{\mathfrak{a}}\cdot\frac{\mathfrak{b}_1}{\mathfrak{a}_1} > \frac{\mathfrak{bb}_1}{\mathfrak{aa}_1}.$$

If, however, $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{a}_1$, $\mathfrak{b}_1$ are four ideals, then

$$\frac{\mathfrak{b}}{\mathfrak{a}}\cdot\frac{\mathfrak{b}_1}{\mathfrak{a}_1} = \frac{\mathfrak{bb}_1}{\mathfrak{aa}_1}.$$

For

$$\frac{\mathfrak{b}}{\mathfrak{a}}\cdot\frac{\mathfrak{b}_1}{\mathfrak{a}_1} = \mathfrak{ba}^{-1}\mathfrak{b}_1\mathfrak{a}^{-1} = \mathfrak{bb}_1\mathfrak{a}^{-1}\mathfrak{a}_1^{-1} = \mathfrak{bb}_1(\mathfrak{aa}_1)^{-1} = \frac{\mathfrak{bb}_1}{\mathfrak{aa}_1}.$$

[1] Vol. I, Art. 125.
[2] Vol. I, Art. 131.

If $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{b}_1$, $\mathfrak{a}_1$ are four ideals, we further have

$$\frac{\frac{\mathfrak{b}}{\mathfrak{a}}}{\frac{\mathfrak{b}_1}{\mathfrak{a}_1}} = \frac{\mathfrak{b}\mathfrak{a}_1}{\mathfrak{a}\mathfrak{b}_1}.$$

We may first prove the important theorem that

$$\frac{\mathfrak{o}}{\frac{\mathfrak{b}}{\mathfrak{a}}} = \frac{\mathfrak{a}}{\mathfrak{b}}.$$

From the preceding article,

$$\frac{\mathfrak{o}}{\frac{\mathfrak{b}}{\mathfrak{a}}} = \left(\frac{\mathfrak{b}}{\mathfrak{a}}\right)^{-1} = (\mathfrak{b}\mathfrak{a}^{-1})^{-1} = \mathfrak{b}^{-1}\mathfrak{a} = \frac{\mathfrak{a}}{\mathfrak{b}}.$$

Hence, it follows that

$$\frac{\frac{\mathfrak{b}}{\mathfrak{a}}}{\frac{\mathfrak{b}_1}{\mathfrak{a}_1}} = \frac{\mathfrak{b}}{\mathfrak{a}} \cdot \frac{\mathfrak{o}}{\frac{\mathfrak{b}_1}{\mathfrak{a}_1}} = \frac{\mathfrak{b}}{\mathfrak{a}} \cdot \frac{\mathfrak{a}_1}{\mathfrak{b}_1} = \frac{\mathfrak{b}\mathfrak{a}_1}{\mathfrak{a}\mathfrak{b}_1}.$$

If $\mathfrak{d} = \mathfrak{a} + \mathfrak{b} + \mathfrak{c} + \cdots$, then $\mathfrak{d}^{-1} = \mathfrak{a}^{-1} - \mathfrak{b}^{-1} - \mathfrak{c}^{-1} - \cdots$; and if $\mathfrak{m} = \mathfrak{a} - \mathfrak{b} - \mathfrak{c} - \cdots$, then $\mathfrak{m}^{-1} = \mathfrak{a}^{-1} + \mathfrak{b}^{-1} + \mathfrak{c}^{-1} + \cdots$.

We shall prove these two theorems for the case of two ideals, but it is evident that they may be extended to the case of three or more ideals. Suppose that $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals and that $\mathfrak{d} = \mathfrak{a} + \mathfrak{b}$, so that $\mathfrak{d}$ is also an ideal. From Formula VI, Vol. I, Art. 131, it is seen that

$$\frac{\mathfrak{o}}{\mathfrak{d}} = \frac{\mathfrak{o}}{\mathfrak{a}} - \frac{\mathfrak{o}}{\mathfrak{b}} \qquad \text{or} \qquad \mathfrak{d}^{-1} = \mathfrak{a}^{-1} - \mathfrak{b}^{-1} = [\mathfrak{a} + \mathfrak{b}]^{-1}.$$

If further

$$\mathfrak{x} = \mathfrak{a}^{-1} + \mathfrak{b}^{-1},$$

then from the theorem just proved,

$$\mathfrak{x}^{-1} = (\mathfrak{a}^{-1})^{-1} - (\mathfrak{b}^{-1})^{-1} = \mathfrak{a} - \mathfrak{b} = \mathfrak{m}.$$

Hence,

$$[\mathfrak{a}-\mathfrak{b}]^{-1}=[\mathfrak{x}^{-1}]^{-1}=\mathfrak{x}=\mathfrak{a}^{-1}+\mathfrak{b}^{-1}.$$

In general we have

$$(\mathfrak{a}+\mathfrak{b}+\mathfrak{c}+\cdots)^{-1}=\mathfrak{a}^{-1}-\mathfrak{b}^{-1}-\mathfrak{c}^{-1}-\cdots,$$
$$(\mathfrak{a}-\mathfrak{b}-\mathfrak{c}-\cdots)^{-1}=\mathfrak{a}^{-1}+\mathfrak{b}^{-1}+\mathfrak{c}^{-1}+\cdots.$$

Using these formulas we may again render complete other formulas in the general modul theory, namely,

If $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{d}$, $\mathfrak{m}$ are ideals,

(1) $\mathfrak{c}\mathfrak{d}=\mathfrak{c}\mathfrak{a}+\mathfrak{c}\mathfrak{b}$ (Vol. I, Art. 127);

(2) $\mathfrak{c}\mathfrak{m}=\mathfrak{c}\mathfrak{a}-\mathfrak{c}\mathfrak{b}$ (Vol. I, Art. 128);

(3) $\mathfrak{d}\mathfrak{m}=\mathfrak{a}\mathfrak{b}$ (Vol. I, Art. 128).

Since the first theorem is true for moduls in general, it need not be considered further here.

To prove (2) observe from above that

$$\mathfrak{m}^{-1}=\mathfrak{a}^{-1}+\mathfrak{b}^{-1}$$
$$\mathfrak{m}^{-1}\mathfrak{c}^{-1}=\mathfrak{a}^{-1}\mathfrak{c}^{-1}+\mathfrak{b}^{-1}\mathfrak{c}^{-1}=(\mathfrak{a}\mathfrak{c})^{-1}+(\mathfrak{b}\mathfrak{c})^{-1}$$

and consequently

$$\mathfrak{m}\mathfrak{c}=\mathfrak{a}\mathfrak{c}-\mathfrak{b}\mathfrak{c}.$$

For the proof of (3), we have

$$\mathfrak{m}^{-1}=\mathfrak{a}^{-1}+\mathfrak{b}^{-1},$$

so that

$$\mathfrak{m}^{-1}\mathfrak{a}\mathfrak{b}=(\mathfrak{a}^{-1}+\mathfrak{b}^{-1})\mathfrak{a}\mathfrak{b}=\mathfrak{a}^{-1}\mathfrak{a}\mathfrak{b}+\mathfrak{a}\mathfrak{b}^{-1}\mathfrak{b}=\mathfrak{b}+\mathfrak{a}=\mathfrak{d}.$$

Hence it follows that

$$\mathfrak{a}\mathfrak{b}=\mathfrak{m}\mathfrak{d}.$$

ART. 11. If $\mathfrak{a}$ is an arbitrary modul of the nth order in a realm Ω of the nth degree, and if η is an arbitrary number of this realm, it was proved (Vol. I, Art. 167) that

$$\frac{(\mathfrak{a},\ \mathfrak{a}\eta)}{(\mathfrak{a}\eta,\ \mathfrak{a})}=|N(\eta)|.$$

If we put $\mathfrak{a}=\mathfrak{o}$, it is evident that

$$\frac{(\mathfrak{o},\ \mathfrak{o}\eta)}{(\mathfrak{o}\eta,\ \mathfrak{o})}=|N(\eta)|.$$

This property of the principal order-modul $\mathfrak{o}$ leads to the following definition: *If* $\mathfrak{a}$ *is an arbitrary ideal,* $N(\mathfrak{a})$ *is defined through the formula*

$$N(\mathfrak{a}) = \frac{(\mathfrak{o}, \mathfrak{a})}{(\mathfrak{a}, \mathfrak{o})}.$$

Thus the norm of any arbitrary ideal is a positive *rational* number.

Suppose that the n independent quantities $\omega_1, \omega_2, \cdots, \omega_n$ form a basis of $\mathfrak{o}$, and consequently also a basis of Ω. Further, let $\alpha_1, \alpha_2, \cdots, \alpha_n$ be a basis of an arbitrary ideal $\mathfrak{a}$ in Ω, where Ω is a realm of the nth degree. It follows that

$$\alpha_r = a_{r1}\omega_1 + a_{r2}\omega_2 + \cdots + a_{rn}\omega_n \quad (r = 1, 2, \cdots, n),$$

where $a_{r1}, a_{r2}, \cdots, a_{rn}$ are integral or fractional rational numbers.

If the determinant $|a_{rs}|$ is denoted by A, it is seen (Vol. I, Art. 153) that

$$|A| = \frac{(\mathfrak{o}, \mathfrak{a})}{(\mathfrak{a}, \mathfrak{o})} = N(\mathfrak{a}).$$

We also saw (Vol. I, Art. 94) that

$$\Delta(\mathfrak{a}) = A^2\Delta(\mathfrak{o}) = A^2D,$$

where $D = \Delta(\mathfrak{o})$ is the *basal invariant* in Ω, this invariant being the fundamental discriminant, and that is, the discriminant of $\omega_1, \omega_2, \cdots, \omega_n$ (Vol. I, Art. 94). We therefore have

$$\Delta(\mathfrak{a}) = A^2\Delta(\mathfrak{o}) = N(\mathfrak{a})^2\Delta(\mathfrak{o}) = N(\mathfrak{a})^2D;$$

and consequently

$$N(\mathfrak{a}) = +\sqrt{\frac{\Delta(\mathfrak{a})}{D}} = +\sqrt{\frac{\Delta(\mathfrak{a})}{\Delta(\mathfrak{o})}}.$$

A more general formula may be derived as follows: In Vol. I, Art. 140, we found that

$$(\mathfrak{o}, \mathfrak{a})(\mathfrak{a}, \mathfrak{b})(\mathfrak{b}, \mathfrak{o}) = (\mathfrak{o}, \mathfrak{b})(\mathfrak{b}, \mathfrak{a})(\mathfrak{a}, \mathfrak{o}),$$

or

$$\frac{(\mathfrak{a}, \mathfrak{b})}{(\mathfrak{b}, \mathfrak{a})} = \frac{\dfrac{(\mathfrak{o}, \mathfrak{b})}{(\mathfrak{b}, \mathfrak{o})}}{\dfrac{(\mathfrak{o}, \mathfrak{a})}{(\mathfrak{a}, \mathfrak{o})}} = \frac{N(\mathfrak{b})}{N(\mathfrak{a})}.$$

This formula is also a generalization of the definition of $N(\mathfrak{a})$. For, if we write in this formula $\mathfrak{a} = \mathfrak{o}$, we have

$$\frac{(\mathfrak{o}, \mathfrak{b})}{(\mathfrak{b}, \mathfrak{o})} = \frac{N(\mathfrak{b})}{N(\mathfrak{o})} = N(\mathfrak{b}),$$

since

$$N(\mathfrak{o}) = \frac{(\mathfrak{o}, \mathfrak{o})}{(\mathfrak{o}, \mathfrak{o})} = 1.$$

Other generalizations of this formula for $N(\mathfrak{a})$ may be had as follows: Let $\mathfrak{a} = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ and $\mathfrak{b} = (\beta_1, \beta_2, \cdots, \beta_n)$ be two ideals in Ω. As their respective elements form two bases in this realm, we must have

$$\beta_r = c_{r1}\alpha_1 + c_{r2}\alpha_2 + \cdots + c_{rn}\alpha_n \quad (r = 1, 2, \cdots, n),$$

where $c_{r1}, c_{r2}, \cdots, c_{rn}$ are integral or fractional rational numbers. If we put $|c_{rs}| = C$, we have (Vol. I, Art. 153),

$$|C| = \frac{(\mathfrak{a}, \mathfrak{b})}{(\mathfrak{b}, \mathfrak{a})} = \frac{N(\mathfrak{b})}{N(\mathfrak{a})}.$$

From Vol. I, Arts. 64, 144, we found that

$$\Delta(\beta_1, \beta_2, \cdots, \beta_n) = C^2\Delta(\alpha_1, \alpha_2, \cdots, \alpha_n);$$

and consequently

$$\frac{\Delta(\mathfrak{b})}{\Delta(\mathfrak{a})} = \left(\frac{N(\mathfrak{b})}{N(\mathfrak{a})}\right)^2.$$

If the special case of the principal ideals be considered, we have

$$N(\mathfrak{o}\eta) = |N(\eta)|;$$

for

$$\frac{\Delta(\mathfrak{o}\eta)}{\Delta(\mathfrak{o})} = \left(\frac{N(\mathfrak{o}\eta)}{N(\mathfrak{o})}\right)^2.$$

Then observe that

$$\Delta(\mathfrak{o}\eta) = N(\eta^2)\Delta(\mathfrak{o}) \qquad \text{and} \qquad N(\mathfrak{o}) = 1.$$

If finally $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals, and if $\mathfrak{b} > \mathfrak{a}$, so that $(\mathfrak{b}, \mathfrak{a}) = 1$, then is

$$\frac{N(\mathfrak{b})}{N(\mathfrak{a})} = (\mathfrak{a}, \mathfrak{b}).$$

Consequently $N(\mathfrak{b})$ is divisible by $N(\mathfrak{a})$, if $\mathfrak{b}$ is divisible by $\mathfrak{a}$. The inverse of this theorem is *not* true.

CHAPTER II

INTEGRAL IDEALS

ART. **12. Definition.** An ideal is said to be *integral*, if it consists only of algebraic integers.

In every such ideal i there are always n integers $\iota_1, \iota_2, \cdots, \iota_n$, which have the property that every number (integer) γ of the ideal may be expressed in the form

$$\gamma = a_1\iota_1 + a_2\iota_2 + \cdots + a_n\iota_n,$$

where the a's are rational integers.

To prove this, let $k_0, k_1, k_2, \cdots$ denote rational integers; and write down all numbers of the ideal which have the form

$$\begin{aligned}
\gamma k_0 &= a_{10}\omega_1 + a_{20}\omega_2 + \cdots + a_{k0}\omega_k, \\
\gamma k_1 &= a_{11}\omega_1 + a_{21}\omega_2 + \cdots + a_{k1}\omega_k, \\
\gamma k_2 &= a_{12}\omega_1 + a_{22}\omega_2 + \cdots + a_{k2}\omega_k, \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots
\end{aligned}$$

where the a's are rational integers, and the ω's are the basis of all integers of Ω.

Let a_k be the greatest common divisor of $a_{k0}, a_{k1}, a_{k2}, \cdots$, so that ($A_{k0}, A_{k1}, \cdots$, denoting definite rational integers)

$$A_{k0}a_{k0} + A_{k1}a_{k1} + A_{k2}a_{k2} + \cdots = a_k;$$

and put (the b's being rational integers)

$$\begin{aligned}
\iota_k &= A_{k0}\gamma k_0 + A_{k1}\gamma k_1 + A_{k2}\gamma k_2 + \cdots \\
&= b_{1k}\omega_1 + b_{2k}\omega_2 + \cdots + a_k\omega_k \\
&\qquad (k = 1, 2, \cdots, n).
\end{aligned}$$

It follows as in Vol. I, Art. 96, that $\iota_1, \iota_2, \cdots, \iota_n$ are the n integers having the required property.

ART. **13.** If $\mathfrak{a}$ and $\mathfrak{b}$ are two integral ideals, then $\mathfrak{a}+\mathfrak{b}$, $\mathfrak{a}-\mathfrak{b}$ and $\mathfrak{ab}$ are integral ideals. The quotient of two integral ideals $\frac{\mathfrak{b}}{\mathfrak{a}}$ is an integral ideal only when $\mathfrak{b} > \mathfrak{a}$. For, if the quotient of two ideals $\frac{\mathfrak{b}}{\mathfrak{a}}$ is equal to an integral ideal $\mathfrak{g}$, then

$$\mathfrak{a}\frac{\mathfrak{b}}{\mathfrak{a}} = \mathfrak{ag}, \qquad \text{or} \qquad \mathfrak{ag} = \mathfrak{b}.$$

If, however, $\mathfrak{g}$ is an integral ideal, then is

$$\mathfrak{g} > \mathfrak{o},$$

and consequently

$$\mathfrak{ag} > \mathfrak{ao} > \mathfrak{a}, \qquad \text{or} \qquad \mathfrak{b} > \mathfrak{a}.$$

Inversely, if $\mathfrak{b} > \mathfrak{a}$, where $\mathfrak{b}$ and $\mathfrak{a}$ are ideals, then $\frac{\mathfrak{b}}{\mathfrak{a}}$ is an integral ideal. For, it was shown in Vol. I, Art. 161 that if $\mathfrak{b} > \mathfrak{a}$, where $\mathfrak{a}$ is a finite modul, the modul $\frac{\mathfrak{b}}{\mathfrak{a}}$ consists only of algebraic integers. Thus, while the first part of the assertion is true only for ideals, the second is true for arbitrary finite moduls.

Next suppose that $\mathfrak{a}$ is an ideal and let α be a number divisible by $\mathfrak{a}$. Then is $\alpha\mathfrak{o} > \mathfrak{a}$ and consequently also $\frac{\alpha\mathfrak{o}}{\mathfrak{a}}$ is equal to an integral ideal, say $\mathfrak{g}$, so that

$$\mathfrak{ag} = \alpha\mathfrak{o}.$$

We thus have the theorem: *Every ideal* $\mathfrak{a}$ *may, through multiplication by an* integral *ideal, be transformed into a principal ideal, and further, the number* α *which produces the principal ideal is divisible by* $\mathfrak{a}$.

In the theorem of Art. 8, Vol. II,[1] we saw that associated with every ideal $\mathfrak{a}$ there was another ideal $\mathfrak{b}$ such that $\mathfrak{ab} = \mathfrak{o}$, and from this it follows that every ideal can by multiplication with a second ideal (not necessarily

[1] Vol. II will hereafter be omitted when reference is made to the present volume.

integral) be transformed into a principal ideal. What is new in the above theorem is the fact that the ideal $\mathfrak{a}$ is multiplied by an *integral* ideal and thereby produces a principal ideal.

ART. **14. The Primary Theorem.** The fact that every integral ideal $\mathfrak{i}$ may be multiplied by another integral ideal $\mathfrak{i}_1$ so chosen that $\mathfrak{i}\mathfrak{i}_1 = \mathfrak{o}\iota$, where $\mathfrak{o}\iota$ is a principal ideal, must be made fundamental in the general theory of ideals. For with the proof of this theorem a second theorem may be proved, namely, if $\mathfrak{c} > \mathfrak{a}$, where $\mathfrak{c}$ and $\mathfrak{a}$ are integral ideals, a third integral ideal $\mathfrak{b}$ may be found such that $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$. Reciprocally, if the latter theorem is proved, the former theorem follows; for, if α is any integer in $\mathfrak{i}$, then the ideal $\mathfrak{o}\alpha$ is divisible by $\mathfrak{i}$. And, admitting the second theorem, it follows at once that $\mathfrak{o}\alpha = \mathfrak{i}\mathfrak{i}_1$, which is the first theorem. Further, if $\mathfrak{c} > \mathfrak{a}$, then $\mathfrak{c}\mathfrak{i} > \mathfrak{a}\mathfrak{i}$ for every ideal $\mathfrak{i}$. And admitting the first theorem, namely, $\mathfrak{a}\mathfrak{i} = \mathfrak{o}\alpha$, it follows that there exists an ideal $\mathfrak{i}$ such that $\mathfrak{i}\mathfrak{c} > \mathfrak{o}\alpha$. It then follows that all the integers of $\mathfrak{c}\mathfrak{i}$ are of the form $\omega\alpha$, the ω's being integers in $\mathfrak{o}$. And the collectivity $\mathfrak{b}$ of these integers $\omega\alpha$, which correspond to integers of $\mathfrak{c}\mathfrak{i}$, form an ideal. To prove this we have only (Art. 4) to show that the condition $\mathfrak{o}\mathfrak{b} = \mathfrak{b}$ is satisfied. Let ω_1 be any other integer in $\mathfrak{o}$; then is $\omega_1 \cdot \omega\alpha = \omega_1\omega \cdot \alpha$ an integer in $\mathfrak{c}\mathfrak{i}$, if $\omega\alpha$ is such an integer. Hence, $\omega_1\omega$ is an integer in $\mathfrak{b}$. Multiplying the equality $\mathfrak{c}\mathfrak{i} = \mathfrak{b}\alpha$ by $\mathfrak{a}$ we have $\mathfrak{a}\mathfrak{c}\mathfrak{i} = \mathfrak{a}\mathfrak{b}\alpha$; and since $\mathfrak{a}\mathfrak{i} = \mathfrak{o}\alpha$, it follows finally that $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$.

Hence, in the proof of the theorem, namely, *if* $\mathfrak{c} > \mathfrak{a}$, *there exists an ideal* $\mathfrak{b}$ *such that* $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$, we may confine our attention to the proof of the first theorem, namely: *Corresponding to any ideal* $\mathfrak{i}$ *there exists a second ideal* $\mathfrak{i}_1$ *whose product is a principal ideal.*

Either of these two theorems, which have the same content, will be referred to as the *Primary Theorem.*

Preliminary to the proof of this theorem we must prove a lemma, upon which depends a generalization of the *Gaussian Theorem* of Vol. I, Art. 4.

With Dedekind [1] let

$$f(x) = c_0x^s + c_1x^{s-1} + \cdots + c_{s-1}x + c_s$$

be an integral function of x with integral algebraic coefficients and let ω be a root of the equation

$$f(x) = 0.$$

Further, write

$$C_i = c_0\omega^i + c_1\omega^{i-1} + \cdots + c_i \quad (i = 0, 1, 2, \cdots, s);$$

and observe that

$$C_{i+1} - C_i\omega = c_{i+1}$$

is a recursion formula, through which the capital C's may be expressed through the small c's with $C_0 = c_0$.

Due to the fact that

$$c_0\omega^s + c_1\omega^{s-1} + \cdots + c_s = 0,$$

we have at once

$$\begin{aligned}
C_i &= c_0\omega^i + c_1\omega^{i-1} + \cdots + c_i, \\
C_i\omega &= c_0\omega^{i+1} + c_1\omega^i + \cdots + c_i\omega, \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
C_i\omega^{s-i-1} &= c_0\omega^{s-1} + c_1\omega^{s-2} + \cdots + c_i\omega^{s-i-1}, \\
C_i\omega^{s-i} &= -c_{i+1}\omega^{s-i-1} - c_{i+2}\omega^{s-i-2} - \cdots - c_s, \\
C_i\omega^{s-i+1} &= -c_{i+1}\omega^{s-i} - c_{i+2}\omega^{s-i-1} - \cdots - c_s\omega, \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
C_i\omega^{s-1} &= -c_{i+1}\omega^{s-2} - c_{i+2}\omega^{s-3} - \cdots - c_s\omega^{i-1}, \\
C_i\omega^s &= -c_{i+1}\omega^{s-1} - c_{i+2}\omega^{s-2} - \cdots - c_s\omega^i.
\end{aligned}$$

From the first s of these equations we have $C_i\omega^k (k = 0, \cdots, s-1)$ expressed through the quantities $c\omega^k$, where the c's are algebraic integers; and, eliminating $1, \omega, \omega^2, \cdots,$

[1] R. Dedekind, "Ueber einen arithmetischen Satz von Gauss," *Deutsch. Math. Ges. in Prag.*, 1892; *Werke*, Vol. II, p. 28.

ω^{s-1} from these equations, it follows as in Vol. I, Art. 52 that $C_i (i=0, 1, \cdots, s)$ are algebraic integers. Omitting the expression for C_i in the first row of the scheme above and taking the other quantities $C_i\omega^k (k=1, 2, \cdots, s)$, it follows in like manner that $C_i\omega$ are algebraic integers $(i=0, 1, \cdots, s)$.

Observing *first* that

$$\frac{f(x)}{x-\omega} = C_0x^{s-1}+C_1x^{s-2}+\cdots+C_{s-1},$$

it is seen that the coefficients C are algebraic integers.

Next let

$$\mathfrak{m}=[\alpha, \beta]$$

be a modul of two elements in which α and β are algebraic numbers. It follows that $\omega=\frac{\alpha}{\beta}$ is also an algebraic number and therefore satisfies an algebraic equation whose coefficients, say c_i, are rational integers. The greatest common divisor of the c's is unity; and that is,

$$[c_0, c_1, \cdots, c_s]=[1]=\mathfrak{z},$$

where the modul $\mathfrak{z}$ consists of all rational integers.

Write $C_i=\beta\nu_i$ so that $C_i\omega=\alpha\nu_i$. It follows from above that $\beta\nu_i$ and $\alpha\nu_i$ are algebraic integers. Also from above it is seen that

$$C_0=\beta\nu_0=c_0 \quad \text{and} \quad \beta\nu_{i+1}-\alpha\nu_i=c_{i+1} \quad [i=1, 2, \cdots].$$

From these formulas we may express rationally the quantities $\nu_0, \nu_1, \cdots, \nu_s$ in terms of α and β.

Writing

$$\mathfrak{n}=[\nu_0, \nu_1, \cdots, \nu_s],$$

it is clear that the product of this modul by $\mathfrak{m}$, and that is, $\mathfrak{m}\mathfrak{n}=[\cdots, \alpha\nu_i, \cdots, \beta\nu_i, \cdots]=[\cdots, \alpha\nu_i, \cdots, \beta\nu_i, \cdots, c_i]$ consists only of algebraic integers and contains also the modul

$$[c_0, c_1, \cdots, c_s]=\mathfrak{z}.$$

With this again is proved the lemma in question: *Every modul* $\mathfrak{m}$, *consisting of two elements which are algebraic integers, may be multiplied by a second modul* $\mathfrak{n}$ *whose elements may be expressed rationally through the elements of* $\mathfrak{m}$, *such that the modul* $\mathfrak{mn}$ *has as elements only algebraic integers including the rational unit 1.*

Extending this theorem as was done in Vol. I, Art. 163, it is seen that *any modul* $\mathfrak{m}$ *consisting of n elements that are algebraic numbers may be multiplied by a second modul* $\mathfrak{n}$ *whose elements may be expressed rationally through the elements of* $\mathfrak{m}$ *and such that the product* $\mathfrak{mn}$ *is a modul, whose elements consist only of algebraic integers including the modul* $[1]=\mathfrak{z}$.

ART. **15. The Generalized Gaussian Theorem.** We are now in a position to prove first the *Gaussian Generalized Theorem* and therefrom the *Primary Theorem.* Writing the functions $A(x)$, $B(x)$, $C(x)$, where $A(x)B(x)=C(x)$, in the form

$$A(x)=a_0(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_m),$$
$$B(x)=b_0(x-\beta_1)(x-\beta_2)\cdots(x-\beta_n),$$
$$C(x)=c_0(x-\omega_1)(x-\omega_2)\cdots(x-\omega_{m+n}),$$

it is seen by a repetition of the theorem of the preceding article, that if the coefficients in $C(x)$ are algebraic integers, the coefficients of the resulting expressions, when $C(x)$ is divided by any number of linear factors $x-\omega_i$, are also algebraic integers. These coefficients, consisting of the sums of products of the form $c_0\omega_i\omega_k\omega_l\cdots$, constitute all the terms of the product

$$c_0(1+\omega_1)(1+\omega_2)\cdots(1+\omega_{m+n}).$$

Further, these terms are identical with the terms in the combined products

$$a_0(1+\alpha_1)(1+\alpha_2)\cdots(1+\alpha_m),$$
$$b_0(1+\beta_1)(1+\beta_2)\cdots(1+\beta_n).$$

And that is, if $c_0\Pi\omega_i$ is any term of the first set, there is a term in the product $a_0\Pi\alpha_j b_0\Pi\beta_k$ which is equal to it.

It follows, since $a_0b_0=c_0$, that the product $\Pi\alpha_j\Pi\beta_k$ is an algebraic integer.

Observing that every coefficient a_j of $A(x)$ is an aggregate of terms of the form $a_0\Pi\alpha_j$, while every coefficient b_k of $B(x)$ is an aggregate of terms of the form $b_0\Pi\beta_k$, the extended Gaussian Theorem is proved, namely: *If the product C of two functions A and B has only integral coefficients, then every product formed of a coefficient of A and a coefficient of B is an integer.*

To prove the Primary Theorem, let

$$\mathfrak{i}=(\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n)$$

be any ideal. Form the function

$$A(x;\ \alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n)=A(x)=\alpha_1x^{n-1}+\alpha_2x^{n-2}+\cdots+\alpha_n;$$

and let

$$B(x)=\beta_1x^{r-1}+\beta_2x^{r-2}+\cdots+\beta_r$$

represent the product $A(x;\ \alpha_1',\ \alpha_2',\ \cdots,\ \alpha_n')(x;\ \alpha_1'',\ \alpha_2'',\ \cdots,\ \alpha_n'')\cdots(x;\ \alpha_1^{(n-1)},\ \cdots,\ \alpha_n^{(n-1)})$, where the coefficients $\beta_1,\ \cdots,\ \beta_r$ belong to the same realm as $\alpha_1,\ \alpha_2,\ \cdots,\ \cdots,\ \alpha_n$.

Denote by $\mathfrak{i}_1$ the ideal $(\beta_1,\ \beta_2,\ \cdots,\ \beta_r)$, an ideal which is uniquely determined when $\mathfrak{i}$ is given. Observe further that

$$A(x)B(x)=C(x)=g_1x^{s-1}+g_2x^{s-2}+\cdots+g_s,$$

where the g's are rational integers.

If g is the greatest common divisor of $g_1,\ g_2,\ \cdots,\ g_s$, it is possible to find such integers k that

$$g=k_1g_1+k_2g_2+\cdots+k_sg_s. \qquad \text{(a)}$$

From the Gaussian Theorem it is seen that the quantities $\alpha_i\beta_j$ are all divisible by g. And that is, $\mathfrak{i}\mathfrak{i}_1>\mathfrak{o}g$. Further, since

$$g_1=\alpha_1\beta_1,\qquad g_2=\alpha_1\beta_2+\alpha_2\beta_1,\qquad g_3=\alpha_1\beta_3+\alpha_2\beta_2+\alpha_3\beta_1,\ \cdots,$$

it follows from (a) that $\mathfrak{o}g$ is divisible by $\mathfrak{i}\mathfrak{i}_1$. And this with the fact that $\mathfrak{i}\mathfrak{i}_1 > \mathfrak{o}g$ shows that

$$\mathfrak{i}\mathfrak{i}_1 = \mathfrak{o}g.$$

With this is proved the Primary Theorem (Art. 14).

ART. **16.** Owing to the importance of the above theorem, we shall give here a second proof also due to Dedekind.[1] Proofs by Hurwitz are found in Chapter V.

If $\mathfrak{i} = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ is an ideal of the stock realm $\Re(\alpha)$, of degree n, it follows from the theorem at the end of Art. 14 that there exists a modul $\mathfrak{m}$, whose elements belong to $\Re(\alpha)$, such that the modul $\mathfrak{i}\mathfrak{m}$ consists only of algebraic integers of the fixed realm and further $[1] = \mathfrak{z}$ is divisible by the modul $\mathfrak{i}\mathfrak{m}$.

Observe on the one hand that

$$\mathfrak{z} > \mathfrak{i}\mathfrak{m} > \mathfrak{o};$$

and on the other, since $\mathfrak{o}\mathfrak{z} = \mathfrak{o}$, that

$$\mathfrak{o}\mathfrak{z} > \mathfrak{o}\mathfrak{i}\mathfrak{m}, \qquad \text{or} \qquad \mathfrak{o} > \mathfrak{i}\mathfrak{m}.$$

It follows that

$$\mathfrak{i}\mathfrak{m} = \mathfrak{o}.$$

Since the order-modul $\mathfrak{i}^0 = \frac{\mathfrak{i}}{\mathfrak{i}}$, like every other order-modul, contains $[1]$ as an element, and as $\mathfrak{o}$ is the only ideal that contains $[1]$, it is seen that $\mathfrak{o} = \mathfrak{i}^0$.

Accordingly, we may write

$$\mathfrak{i}\mathfrak{m} = \mathfrak{i}^0. \tag{1}$$

Next define the complex $\mathfrak{i}_1$ by the relation $\mathfrak{i}_1 = \frac{\mathfrak{i}^0}{\mathfrak{i}}$. It may be proved as follows that $\mathfrak{i}_1\mathfrak{i} = \mathfrak{i}^0$. (Observe that $\mathfrak{i}_1$ is not necessarily an integral ideal.)

[1] Dedekind, *op. cit.* See also J. König, *Einleitung in die allgemeine Theorie der algebraischen Grössen*, 1903, pp. 74 *et seq.*

By the above definition i_1 is the collectivity of all numbers τ such that $i\tau > i^0$. It may be shown first that

$$i^0 i_1 = i_1. \tag{2}$$

For, due to the fact that i^0 contains the modul [1], we have on the one hand $i_1 > i^0 i_1$. On the other hand, since by definition $ii_1 > i^0$, we have $ii^0 i_1 > i^0 i^0 (= i^0)$. And, therefore, as seen from above, ii_0 denotes numbers of the complex τ, so that $i^0 i_1 > i_1$. We accordingly have

$$i^0 i_1 = i_1. \tag{2}$$

Next from (1) it follows through multiplication by i^0 that

$$ii^0 m = i^0;$$

and that is, the numbers of $i^0 m$ are among those numbers τ which constitute i_1 and therefore $i^0 m > i_1$; further, multiplying the expression $ii_1 > i^0$ (given above) by m, and observing the relations (1) and (2), it is seen that $i_1 > i^0 m$.

We have accordingly

$$i_1 = i^0 m.$$

Multiply this equation by i and again use equation (1), it results that

$$ii_1 = i^0 = 0. \tag{3}$$

Next let π denote the product of the basal elements of i so that $\pi = \alpha_1 \alpha_2 \cdots \alpha_n$, and observe that

$$i_1 = \frac{i^0}{i} = \frac{i^0}{\alpha_1} - \frac{i^0}{\alpha_2} - \cdots - \frac{i^0}{\alpha_n}.$$

It follows that the modul $i_1 \pi = i_2$ consists only of integers of the realm.

Further observe that

$$i_2 0 = i_2 i^0 = i_1 \pi i^0,$$

and from (2)

$$i_1 i^0 \pi = i_1 \pi = i_2.$$

And therefore $\mathfrak{i}_2$ is an ideal (Art. 4). Multiplying the equation (3) by π, it follows that

$$\mathfrak{i}\mathfrak{i}_2 = \mathfrak{o}\pi.$$

With this it is again proved directly from the modul-theory, that *corresponding to any given ideal* $\mathfrak{i}$, *there is a second ideal* $\mathfrak{i}_2$, *such that their product is a principal ideal.*

Suppose that $\mathfrak{a}$ is an ideal divisible by the principal ideal $\mathfrak{o}\eta$, that is, $\mathfrak{a} > \mathfrak{o}\eta$. If then α is a number divisible by $\mathfrak{a}$, it follows that $\alpha = \omega\eta$, where ω is an integer divisible by $\mathfrak{o}$; and that is, α is an algebraic integer in Ω. Hence, if $\mathfrak{a} > \mathfrak{o}\eta$, all numbers that are divisible by $\mathfrak{a}$ are divisible by η; and $\mathfrak{a}\eta^{-1}$ is an integral ideal, since it is divisible by $\mathfrak{o}$. From this it is seen that an ideal $\mathfrak{a}$ is divisible by the number η, if all numbers divisible by $\mathfrak{a}$ are divisible by η; or, if $\mathfrak{a}$ is divisible by the principal ideal $\mathfrak{o}\eta$; or, if $\mathfrak{a}\eta^{-1}$ is an integral ideal.

The *norm* of an integral ideal is a *positive* rational integer. For, if $\mathfrak{g}$ is an integral ideal, then $\mathfrak{g} > \mathfrak{o}$, since $\mathfrak{g}$ consists only of algebraic integers in Ω. Hence (Vol. I, Art. 138),

$$(\mathfrak{g}, \mathfrak{o}) = 1$$

and consequently (Art. 11)

$$N(\mathfrak{g}) = \frac{(\mathfrak{o}, \mathfrak{g})}{(\mathfrak{g}, \mathfrak{o})} = (\mathfrak{o}, \mathfrak{g}).$$

ART. 17. **Ideals Relatively Prime.** If $\mathfrak{a}$, $\mathfrak{b}$ are two integral ideals, and if further

$$\mathfrak{d} = \mathfrak{a} + \mathfrak{b}, \qquad \frac{\mathfrak{a}}{\mathfrak{d}} = \mathfrak{a}', \qquad \frac{\mathfrak{b}}{\mathfrak{d}} = \mathfrak{b}',$$

then $\mathfrak{a}'$ and $\mathfrak{b}'$ are integral ideals, because $\mathfrak{a} > \mathfrak{d}$ and $\mathfrak{b} > \mathfrak{d}$. If further $\mathfrak{m} = \mathfrak{a} - \mathfrak{b}$, it follows (Art. 10) that

$$\mathfrak{m}\mathfrak{d} = \mathfrak{a}\mathfrak{b}.$$

Since, however,

$$\mathfrak{a} = \mathfrak{a}'\mathfrak{d} \qquad \text{and} \qquad \mathfrak{b} = \mathfrak{b}'\mathfrak{d},$$

we have

$$\mathfrak{m}\mathfrak{d} = \mathfrak{a}'\mathfrak{b}'\mathfrak{d}\mathfrak{d};$$

or

$$\mathfrak{m} = \mathfrak{a}'\mathfrak{b}'\mathfrak{d} = \mathfrak{a}'\mathfrak{b} = \mathfrak{a}\mathfrak{b}'.$$

If further

$$\mathfrak{d} = \mathfrak{o}, \qquad \text{then} \qquad \mathfrak{m} = \mathfrak{a}\mathfrak{b}.$$

Two integral ideals $\mathfrak{a}$, $\mathfrak{b}$ whose greatest common divisor is $\mathfrak{o}$, are said to be *relatively prime*. In this case the least common multiple is equal to their product.

THEOREM. *If two integral ideals* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are relatively prime, and if* $\mathfrak{c}$ *is a third ideal (integral), then*

$$\mathfrak{a} + \mathfrak{b}\mathfrak{c} = \mathfrak{a} + \mathfrak{c}.$$

For

$$\mathfrak{a} + \mathfrak{b} = \mathfrak{o},$$

and

$$(\mathfrak{a} + \mathfrak{b})\mathfrak{c} = \mathfrak{a}\mathfrak{c} + \mathfrak{b}\mathfrak{c} = \mathfrak{o}\mathfrak{c} = \mathfrak{c};$$

so that

$$\mathfrak{a} + \mathfrak{c} = \mathfrak{a} + (\mathfrak{a}\mathfrak{c} + \mathfrak{b}\mathfrak{c}) = \mathfrak{a} + \mathfrak{a}\mathfrak{c} + \mathfrak{b}\mathfrak{c};$$

and since

$$\mathfrak{a}\mathfrak{c} > \mathfrak{a},$$

it follows that

$$\mathfrak{a} + \mathfrak{c} = \mathfrak{a} + \mathfrak{b}\mathfrak{c}.$$

Consider next two special cases of this important theorem. (1) If $\mathfrak{a}$ and $\mathfrak{b}$ are two integral ideals that are relatively prime, and if $\mathfrak{c}$ is a third ideal, and if further $\mathfrak{b}\mathfrak{c} > \mathfrak{a}$, then also

$$\mathfrak{c} > \mathfrak{a}.$$

For, if

$$\mathfrak{b}\mathfrak{c} > \mathfrak{a}, \quad \text{then also} \quad \mathfrak{a} + \mathfrak{b}\mathfrak{c} = \mathfrak{a}, \quad \text{or} \quad \mathfrak{a} + \mathfrak{c} = \mathfrak{a},$$

and consequently

$$\mathfrak{c} > \mathfrak{a}.$$

(2) If $\mathfrak{a}$ and $\mathfrak{b}$ are two integral ideals that are relatively prime, and if $\mathfrak{a}$ and $\mathfrak{c}$ are two integral ideals that are relatively prime, then is

$$\mathfrak{a} + \mathfrak{b}\mathfrak{c} = \mathfrak{a} + \mathfrak{c} = \mathfrak{o}.$$

In general, if $\mathfrak{a}$, $\mathfrak{a}_1$, $\mathfrak{a}_2$, $\cdots$, and $\mathfrak{b}$, $\mathfrak{b}_1$, $\mathfrak{b}_2$, $\cdots$ are two series of integral ideals, and if every $\mathfrak{b}$ is relatively prime to every $\mathfrak{a}$, then is

$$\mathfrak{a}\mathfrak{a}_1\mathfrak{a}_2\cdots+\mathfrak{b}\mathfrak{b}_1\mathfrak{b}_2\cdots=\mathfrak{o}.$$

ART. **18.** If the integral ideal $\mathfrak{a}$ is divisible by the integral ideal $\mathfrak{g}(\mathfrak{a}>\mathfrak{g})$, so that

$$\frac{\mathfrak{a}}{\mathfrak{g}}=\mathfrak{h}, \text{ or } \mathfrak{a}=\mathfrak{g}\mathfrak{h},$$

where $\mathfrak{h}$ is an integral ideal, the ideal $\mathfrak{g}$ is said to be a *divisor* of $\mathfrak{a}$.

The following theorem may be proved.

THEOREM. *If the integral ideal* $\mathfrak{a}$ *is relatively prime to the integral ideal* $\mathfrak{b}$, *then every divisor of* $\mathfrak{a}$ *is relatively prime to every divisor of* $\mathfrak{b}$.

Since $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime,

$$\mathfrak{a}+\mathfrak{b}=\mathfrak{o}.$$

Let $\mathfrak{a}'$ be a divisor of $\mathfrak{a}$, and $\mathfrak{b}'$ a divisor of $\mathfrak{b}$, so that $\mathfrak{a}'$, $\frac{\mathfrak{a}}{\mathfrak{a}'}$, $\mathfrak{b}'$, $\frac{\mathfrak{b}}{\mathfrak{b}'}$ are integral ideals. Since $\mathfrak{a}>\mathfrak{a}'$ and $\mathfrak{b}>\mathfrak{b}'$, it follows that

$$\mathfrak{a}+\mathfrak{b}>\mathfrak{a}'+\mathfrak{b}',$$

and consequently

$$\mathfrak{o}>\mathfrak{a}'+\mathfrak{b}'.$$

On the other hand, since $\mathfrak{a}'$ and $\mathfrak{b}'$ are integral ideals,

$$\mathfrak{a}'+\mathfrak{b}'>\mathfrak{o}.$$

From this it is seen that

$$\mathfrak{a}'+\mathfrak{b}'=\mathfrak{o},$$

or $\mathfrak{a}'$ is relatively prime to $\mathfrak{b}'$.

Suppose next that the two principal ideals $\mathfrak{o}\alpha$ and $\mathfrak{o}\beta$ (α and β integers) are relatively prime, and that is, let

$$\mathfrak{o}\alpha+\mathfrak{o}\beta=\mathfrak{o}.$$

If further ω is an arbitrary integer in Ω and consequently

divisible by $\mathfrak{o}$, then is

$$\omega = \alpha\xi + \beta\eta,$$

where ξ and η are algebraic integers in Ω. Further, since 1 is an integer in Ω, we have also

$$1 = \alpha\bar{\xi} + \beta\bar{\eta},$$

where $\bar{\xi}$ and $\bar{\eta}$ are integers in Ω.

Reciprocally, if there are two numbers $\bar{\xi}$ and $\bar{\eta}$ divisible by $\mathfrak{o}$, and such that

$$\alpha\bar{\xi} + \beta\bar{\eta} = 1,$$

then $\mathfrak{o}\alpha$ and $\mathfrak{o}\beta$ are relatively prime. For, $\alpha\bar{\xi}$ is divisible by $\alpha\mathfrak{o}$, and $\beta\bar{\eta}$ is divisible by $\beta\mathfrak{o}$, so that $\alpha\bar{\xi}+\beta\bar{\eta}$, that is, 1, is divisible by $\mathfrak{o}\alpha+\mathfrak{o}\beta$. It follows that

$$\mathfrak{o}1 \quad \text{or} \quad \mathfrak{o} > \mathfrak{o}\alpha + \mathfrak{o}\beta.$$

On the other hand, since $\mathfrak{o}\alpha$ and $\mathfrak{o}\beta$ are integral ideals, $\mathfrak{o}\alpha+\mathfrak{o}\beta > \mathfrak{o}$, and consequently $\mathfrak{o}\alpha+\mathfrak{o}\beta = \mathfrak{o}$, and that is, $\mathfrak{o}\alpha$ and $\mathfrak{o}\beta$ are relatively prime.

The following definition may now be offered. Two algebraic integers α and β of the realm Ω are said to be *relatively prime*, if the two principal ideals $\mathfrak{o}\alpha$ and $\mathfrak{o}\beta$ are relatively prime. In virtue of what was given above, this definition has the same significance as the following definition: Two algebraic integers in Ω, say α and β, are *relatively prime*, if in Ω there are two integers ξ and η, such that

$$\alpha\xi + \beta\eta = 1.$$

This conception of two numbers being relatively prime is completely independent of the realm Ω, the only condition being that ξ, η must belong to the same realm as do α, β. From this it is seen that if α and β are relatively prime in any realm of rationality, they are relatively prime in every realm to which α and β both belong.

Having thus defined what is meant when we say that two ideals are relatively prime, or when two algebraic

integers are relatively prime, we may next define what is meant by saying that an algebraic integer is relatively prime to an integral ideal, where the integer and the ideal both belong to Ω.

An algebraic integer β of the realm Ω is said to be relatively prime to the integral ideal $\mathfrak{a}$ in Ω, if the principal ideal $\mathfrak{o}\beta$ is relatively prime to $\mathfrak{a}$.

An ideal is *integral* if it is divisible by $\mathfrak{o}$. All ideals which are not integral are called *fractional.* Any fractional ideal may be made integral as follows. Let $\mathfrak{r}=(\rho_1, \rho_2, \cdots, \rho_n)$ be a fractional ideal, where $\rho_1, \rho_2, \cdots, \rho_n$ are fractional numbers of Ω. Then, since there are always rational integers (Vol. I, Art. 93), say r_ν, such that $r_\nu \cdot \rho_\nu (\nu = 1, 2, \cdots, n)$ are algebraic integers, it is clear that there is a rational integer g, such that $g\mathfrak{r}=\mathfrak{h}$, where $\mathfrak{h} > \mathfrak{o}$. Since $\mathfrak{h}$ is an ideal, we have

$$\mathfrak{o}g\mathfrak{r} = \mathfrak{o}\mathfrak{h} = \mathfrak{h},$$

so that

$$\mathfrak{r} = \frac{\mathfrak{h}}{\mathfrak{o}g}.$$

Further, if $\mathfrak{c}$ is an arbitrary integral ideal,

$$\mathfrak{r} = \frac{\mathfrak{h}}{\mathfrak{o}g} = \frac{\mathfrak{h}\mathfrak{c}}{\mathfrak{o}g\mathfrak{c}} = \frac{\mathfrak{h}\mathfrak{c}}{g\mathfrak{c}} = \frac{\mathfrak{a}}{\mathfrak{b}},$$

where

$$\mathfrak{a} = \mathfrak{h}\mathfrak{c}, \qquad \mathfrak{b} = g\mathfrak{c}.$$

From this it is seen that every ideal may be expressed as the quotient of two integral ideals in an infinite number of ways. Let $\mathfrak{a}+\mathfrak{b}=\mathfrak{d}$, so that

$$\mathfrak{a} = \mathfrak{d}\mathfrak{a}' \qquad \text{and} \qquad \mathfrak{b} = \mathfrak{d}\mathfrak{b}',$$

where $\mathfrak{a}'$ and $\mathfrak{b}'$ are integral ideals that are relatively prime. We then have from the formula just written

$$\mathfrak{r} = \frac{\mathfrak{a}'\mathfrak{d}}{\mathfrak{b}'\mathfrak{d}} = \frac{\mathfrak{a}'}{\mathfrak{b}'}.$$

From this it is seen that every ideal may be expressed as the quotient of two integral ideals that are relatively prime. This expression of an ideal through the quotient of two integral ideals that are relatively prime is unique. For, suppose that $\mathfrak{a} = \frac{\mathfrak{b}}{\mathfrak{a}} = \frac{\mathfrak{b}_1}{\mathfrak{a}_1}$ ($\mathfrak{b}$, $\mathfrak{a}$, $\mathfrak{b}_1$, $\mathfrak{a}_1$ integral). We then have

$$\mathfrak{b}\mathfrak{a}_1 = \mathfrak{a}\mathfrak{b}_1;$$

and consequently

$$\mathfrak{a}\mathfrak{b}_1 > \mathfrak{a}_1.$$

And, as $\mathfrak{a}_1$ and $\mathfrak{b}_1$ are relatively prime, it is seen that $\mathfrak{a} > \mathfrak{a}_1$. Similarly it follows that

$$\mathfrak{b} > \mathfrak{b}_1.$$

Further, if $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime, it follows in the same way that

$$\mathfrak{a}_1 > \mathfrak{a} \qquad \text{and} \qquad \mathfrak{b}_1 > \mathfrak{b},$$

and consequently

$$\mathfrak{a} = \mathfrak{a}_1 \qquad \text{and} \qquad \mathfrak{b} = \mathfrak{b}_1.$$

Next suppose that α is a number divisible by the integral ideal $\mathfrak{a}$, so that therefore $\mathfrak{o}\alpha > \mathfrak{a}$, and consequently $\frac{\mathfrak{o}\alpha}{\mathfrak{a}}$ is equal to an integral ideal, say $\mathfrak{c}$. It follows that

$$\mathfrak{o}\alpha = \mathfrak{a}\mathfrak{c} \qquad \text{and from above} \qquad \mathfrak{r} = \frac{\mathfrak{b}}{\mathfrak{a}} = \frac{\mathfrak{b}\mathfrak{c}}{\mathfrak{a}\mathfrak{c}} = \frac{\mathfrak{b}\mathfrak{c}}{\mathfrak{o}\alpha}.$$

From this it is evident that every ideal $\mathfrak{r}$ may be expressed as the quotient of two integral ideals in an infinite number of ways such that the denominator is always a principal ideal. As $\mathfrak{r} = \frac{\mathfrak{b}\mathfrak{c}}{\mathfrak{o}\alpha}$, it follows that

$$\mathfrak{r}\mathfrak{o}\alpha = \mathfrak{b}\mathfrak{c}, \qquad \text{or} \qquad \alpha\mathfrak{r} = \mathfrak{b}\mathfrak{c}.$$

And since $\mathfrak{b}$ and $\mathfrak{c}$ are both integral, $\alpha\mathfrak{r} > \mathfrak{o}$. This is true of every α, where $\alpha > \mathfrak{a}$ and $\mathfrak{r} = \frac{\mathfrak{b}}{\mathfrak{a}}$ ($\mathfrak{b}$ and $\mathfrak{a}$ integral).

When the ideal $\mathfrak{r}$ is expressed as the quotient of two integral ideals $\frac{\mathfrak{b}}{\mathfrak{a}}$, which are relatively prime, $\mathfrak{a}$ is called the *denominator* and $\mathfrak{b}$ the *numerator* of $\frac{\mathfrak{b}}{\mathfrak{a}}=\mathfrak{r}$. This notation is applied only when the two ideals are relatively prime. The denominator $\mathfrak{a}$ is, as we have just seen, the greatest common divisor of all integers α for which

$$\alpha\mathfrak{r}>\mathfrak{o}, \qquad \text{that is,} \qquad \mathfrak{a}=\alpha\mathfrak{o}+\alpha'\mathfrak{o}+\alpha''\mathfrak{o}+\cdots,$$

where $\alpha\mathfrak{r}>\mathfrak{o}$, $\alpha'\mathfrak{r}>\mathfrak{o}$, $\alpha''\mathfrak{r}>\mathfrak{o}$, etc. On the other hand, $\mathfrak{a}$ is the least common multiple of $\mathfrak{o}$ and $\mathfrak{b}\mathfrak{a}^{-1}$. For

$$\mathfrak{a}=\mathfrak{b}\mathfrak{a}^{-1}, \qquad \text{and therefore} \qquad \mathfrak{a}>\mathfrak{b}\mathfrak{a}^{-1},$$

and as $\mathfrak{a}$ is integral, it follows also that $\mathfrak{a}>\mathfrak{o}$. The numerator $\mathfrak{b}$ is the least common multiple of $\mathfrak{r}\mathfrak{a}$ and $\mathfrak{o}$.

ART. **19. The Norms.** If $\mathfrak{f}$ is an arbitrary modul and if α, β are two arbitrary numbers such that $\alpha-\beta$ is divisible by $\mathfrak{f}$, then (Vol. I, Art. 134) α is said to be *congruent* to β, modulo $\mathfrak{f}$, and we write

$$\alpha\equiv\beta \pmod{\mathfrak{f}}.$$

If $\mathfrak{f}$ is an arbitrary modul, it was seen (Vol. I, Art. 134) that the congruence may be multiplied only by such numbers as are divisible by $\mathfrak{f}$, and still remain a congruence, modulo $\mathfrak{f}$.

If, however, $\mathfrak{f}$ is assumed to be an integral ideal, we may multiply together any two congruences (mod. $\mathfrak{f}$). For example $\mathfrak{f}$ being an integral ideal, if $\alpha\equiv\beta$ (mod. $\mathfrak{f}$), where α and β are integral, and if $\alpha'\equiv\beta'$ (mod. $\mathfrak{f}$), then is $\alpha\alpha'\equiv\beta\beta'$ (mod. $\mathfrak{f}$), where α' and β' are integral. For, if $\alpha\equiv\beta$ (mod. $\mathfrak{f}$), then $\alpha-\beta$ and consequently also $(\alpha-\beta)\omega$, ω being an arbitrary integer in Ω, is divisible by $\mathfrak{f}$. If α' is an algebraic integer, then is $(\alpha-\beta)\alpha'$ divisible by $\mathfrak{f}$, and consequently also

$$(\alpha-\beta)\alpha'+(\alpha'-\beta')\beta=\alpha\alpha'-\beta\beta'$$

is divisible by $\mathfrak{f}$; and that is,

$$\alpha\alpha' \equiv \beta\beta' \pmod{\mathfrak{f}}.$$

If $\mathfrak{f}$ is an integral ideal,[1] then is

$$\mathfrak{f} > \mathfrak{o} \qquad \text{and} \qquad (\mathfrak{f}, \mathfrak{o}) = 1.$$

It follows from Art. 11 that

$$N(\mathfrak{f}) = (\mathfrak{o}, \mathfrak{f}).$$

Or, otherwise expressed $N(\mathfrak{f})$ is equal to the number of incongruent integers (mod. $\mathfrak{f}$) in Ω. As a special case, if $\mathfrak{f}$ is a principal ideal equal to $\mathfrak{o}\kappa$, then (Art. 11)

$$N(\mathfrak{o}, \kappa) = |N(\kappa)|,$$

which is the number of incongruent integers (mod. κ) in Ω.

If $\mathfrak{f}$ is an arbitrary integer ideal, then (Vol. I, Art. 141) is

$$(\mathfrak{o}, \mathfrak{f})\mathfrak{o} = N(\mathfrak{f})\mathfrak{o} > \mathfrak{f}.$$

Hence, for every integer ω in Ω we have

$$N(\mathfrak{f})\omega > \mathfrak{f};$$

and if we put $\omega = 1$, we have $N(\mathfrak{f}) > \mathfrak{f}$, with the resulting theorem:

The norm of an integral ideal is divisible by the ideal.

If k is the smallest rational integer that is divisible by $\mathfrak{f}$, where $\mathfrak{f}$ is an arbitrary integral ideal, then all other rational integers (Vol. I, Art. 170, end) that are divisible by $\mathfrak{f}$ are multiples of k. It follows that $N(\mathfrak{f})$ is divisible by k. On the other hand, the principal ideal $\mathfrak{o}k > \mathfrak{f}$, so that $N(\mathfrak{o}k)$ or k^n is divisible by $N(\mathfrak{f})$. From this it is seen that every prime rational integer which divides either of the two numbers $N(\mathfrak{f})$ or k, divides the other one also, and that a rational integer g which is relatively prime to either of the rational integers $N(\mathfrak{f})$ or k is also relatively prime to the other.

[1] Vol. I, Art. 138.

The following theorem may be proved:

THEOREM. *If a rational integer g is relatively prime to the integral ideal* $\mathfrak{f}$, *it is also relatively prime to* $N(\mathfrak{f})$.

From the remark just made it is necessary only to prove that g is relatively prime to k. The least common multiple of g and k has the form gk', where k' is a rational integer. Every other common multiple of g and k must be divisible by gk'. Hence also gk is divisible by gk', so that k is divisible by k'. On the other hand gk' is divisible by k, and consequently, since k is divisible by $\mathfrak{f}$, it follows that gk' is divisible by $\mathfrak{f}$. But gk' is divisible by $g\mathfrak{o}$, and consequently also by $g\mathfrak{o}-\mathfrak{f}=g\mathfrak{o}\mathfrak{f}=g\mathfrak{f}$. Hence, it is seen that k' is divisible by $\mathfrak{f}$. But all rational integers that are divisible by $\mathfrak{f}$ are multiples of k, so that k' is divisible by k. But we just saw that k was divisible by k'. Hence, it is seen that $k=k'$. It follows that the least common multiple of g and k is gk, so that g and k are relatively prime and consequently g is relatively prime to $N(\mathfrak{f})$.

This theorem may also be proved as follows. Since $\mathfrak{o}g$ and $\mathfrak{f}$ are relatively prime, it follows that

$$\mathfrak{o}g+\mathfrak{f}=\mathfrak{o}.$$

Further, since 1 is divisible by $\mathfrak{o}$, it is also seen that

$$1=g\omega+\kappa,$$

where ω is an integer of $\mathfrak{o}$; and consequently

$$N(\kappa)=N(1-g\omega)=(1-g\omega')(1-g\omega'')\cdots(1-g\omega^{(n)})=1+g\xi,$$

where ξ is an algebraic integer.

On the other hand κ is divisible by $\mathfrak{f}$, so that $N(\kappa)$ is divisible by $N(\mathfrak{f})$ (see end of Art. 11). Hence it follows that

$$N(\kappa)=N(\mathfrak{f})y,$$

where y is a rational integer, and consequently

$$N(\mathfrak{f})y-g\xi=1.$$

From this it is seen first that ξ is a rational number, and being integral, formed of algebraic integers, ξ must be a rational integer. At the same time it follows that g and $N(\mathfrak{f})$ are relatively prime.

ART. 20. LEMMA I. *If* $\mathfrak{a}, \mathfrak{b}_1, \mathfrak{b}_2, \cdots, \mathfrak{b}_r$ *are* $r+1$ *ideals such that* $\mathfrak{a}$ *is divisible by none of the ideals* $\mathfrak{b}_1, \mathfrak{b}_2, \cdots, \mathfrak{b}_r$, *then there is a number* α *which is divisible by* $\mathfrak{a}$ *but by none of the ideals* $\mathfrak{b}_1, \mathfrak{b}_2, \cdots, \mathfrak{b}_r$.

For the case $r=1$, this lemma is true in virtue of the definition of division of one modul by another. The lemma as just stated may be reduced to another form:

Let

$$\mathfrak{m}_s = \mathfrak{a} - \mathfrak{b}_s \qquad (s=1, 2, \cdots, r),$$

so that $\mathfrak{m}_s > \mathfrak{a}$ and $\mathfrak{m}_s > \mathfrak{b}_s$. It is evident that $\mathfrak{a}$ cannot be divisible by $\mathfrak{m}_s$. For if this were true, $\mathfrak{a}$ would be divisible by $\mathfrak{b}_s$, contrary to the hypothesis. It follows that none of the ideals $\mathfrak{m}_1, \mathfrak{m}_2, \cdots, \mathfrak{m}_s$ is equal to $\mathfrak{a}$.

Next write $\frac{\mathfrak{m}_s}{\mathfrak{a}} = \mathfrak{g}_s$, where $\mathfrak{g}_s$ is an integral ideal. Since $\mathfrak{m}_s = \mathfrak{a}\mathfrak{g}_s$, it is seen that none of the ideals $\mathfrak{g}_s$ is the same as $\mathfrak{o}$. For if this were the case then

$$\mathfrak{m}_s = \mathfrak{a}\mathfrak{g}_s = \mathfrak{a}\mathfrak{o} = \mathfrak{a}.$$

Suppose the theorem proved and that the number α is divisible by $\mathfrak{a}$ but by none of the ideals $\mathfrak{b}_s (s=1, 2, \cdots, r)$, then α is also divisible by none of the ideals $\mathfrak{a}\mathfrak{g}_s (s=1, 2, \cdots, r)$. For, if α were divisible by, say $\mathfrak{a}\mathfrak{g}_s = \mathfrak{m}_s$, it would be divisible by $\mathfrak{b}_s$, since $\mathfrak{m}_s > \mathfrak{b}_s$.

Reciprocally, if there is a number α which is divisible by $\mathfrak{a}$ but by none of the ideals $\mathfrak{a}\mathfrak{g}_1, \mathfrak{a}\mathfrak{g}_2, \cdots, \mathfrak{a}\mathfrak{g}_r$, where $\mathfrak{g}_1, \mathfrak{g}_2, \cdots, \mathfrak{g}_r$ are integral ideals that are different from $\mathfrak{o}$, then there is also a number which is divisible by $\mathfrak{a}$ but by none of the ideals $\mathfrak{b}_1, \mathfrak{b}_2, \cdots, \mathfrak{b}_r$. For if there were no such number, then every number divisible by $\mathfrak{a}$ is also

divisible by one of the ideals $\mathfrak{b}_1, \mathfrak{b}_2, \cdots, \mathfrak{b}_r$ and being divisible by $\mathfrak{a}$ is divisible by one of the ideals $\mathfrak{m}_1, \mathfrak{m}_2, \cdots, \mathfrak{m}_r$; and that is, by one of the ideals $\mathfrak{a}\mathfrak{g}_s (s=1, 2, \cdots, r)$. Hence the above lemma has the same significance as the following:

If $\mathfrak{a}$ *is an arbitrary integral or fractional ideal and if* $\mathfrak{g}_1, \mathfrak{g}_2, \cdots, \mathfrak{g}_r$ *are any integral ideals different from* $\mathfrak{o}$, *then there is a number* α *which is divisible by* $\mathfrak{a}$ *but by none of the ideals* $\mathfrak{a}\mathfrak{g}_1, \mathfrak{a}\mathfrak{g}_2, \cdots, \mathfrak{a}\mathfrak{g}_r$.

The case $r=1$, as already remarked, follows by virtue of the definition of divisibility. We may therefore assume the theorem to be proved for the case $r-1$ and under this assumption it may be established for the case r. In the proof two cases are distinguished:

1. If in the series of ideals $\mathfrak{g}_1, \mathfrak{g}_2, \cdots, \mathfrak{g}_r$, there are two ideals that are not relatively prime, say $\mathfrak{g}_1$ and $\mathfrak{g}_2$, so that $\mathfrak{g}_1+\mathfrak{g}_2 \neq \mathfrak{o}$, then in accordance with the assumption, there is a number α which is divisible by $\mathfrak{a}$ but by none of the $r-1$ ideals $\mathfrak{a}(\mathfrak{g}_1+\mathfrak{g}_2), \mathfrak{a}\mathfrak{g}_3, \cdots, \mathfrak{a}\mathfrak{g}_r$. This number α is also divisible by neither $\mathfrak{a}\mathfrak{g}_1$ nor $\mathfrak{a}\mathfrak{g}_2$, for otherwise it would be divisible by $\mathfrak{a}(\mathfrak{g}_1+\mathfrak{g}_2)$. Hence the number α is divisible by $\mathfrak{a}$ but by none of the ideals $\mathfrak{a}\mathfrak{g}_1, \mathfrak{a}\mathfrak{g}_2, \cdots, \mathfrak{a}\mathfrak{g}_r$.

2. Suppose that all the integral ideals $\mathfrak{g}_1, \mathfrak{g}_2, \cdots, \mathfrak{g}_r$ are relatively prime the one to the other. Then $\mathfrak{g}_1$ is also relatively prime to the product $\mathfrak{g}_2\mathfrak{g}_3 \cdots \mathfrak{g}_r$, and consequently also $\mathfrak{a}\mathfrak{g}_2\mathfrak{g}_3 \cdots \mathfrak{g}_r$ is not divisible by $\mathfrak{a}\mathfrak{g}_1$. As the theorem is assumed proved for $r=1$, there is a number α_1 which is divisible by $\mathfrak{a}\mathfrak{g}_2\mathfrak{g}_3 \cdots \mathfrak{g}_r$ but not by $\mathfrak{a}\mathfrak{g}_1$. Similarly there exists a number α_s which is divisible by $\mathfrak{a}\mathfrak{g}_1\mathfrak{g}_2 \cdots \mathfrak{g}_{s-1}\mathfrak{g}_{s+1} \cdots \mathfrak{g}_r$ but which is not divisible by $\mathfrak{a}\mathfrak{g}_s (s=1, 2, \cdots, r)$.

If then we put

$$\alpha = \alpha_1 + \alpha_2 + \cdots + \alpha_r,$$

α satisfies the conditions required in the theorem. For α

is divisible by $\mathfrak{a}$, since, as shown below, $\alpha_1, \alpha_2, \cdots, \alpha_r$ are all divisible by $\mathfrak{a}$. That α_1, say, is divisible by $\mathfrak{a}$ is due to the fact that α_1 is divisible by $\mathfrak{a}\mathfrak{g}_2\mathfrak{g}_3\cdots\mathfrak{g}_r$ and since $\mathfrak{g}_2\mathfrak{g}_3\cdots\mathfrak{g}_r$ is an integral ideal, it follows that $\mathfrak{a}\mathfrak{g}_2\mathfrak{g}_3\cdots\mathfrak{g}_r$ is divisible by $\mathfrak{a}$, and consequently α_1 is divisible by $\mathfrak{a}$. On the other hand α_1 is not divisible by $\mathfrak{a}\mathfrak{g}_1$, while all the other numbers $\alpha_2, \alpha_3, \cdots, \alpha_r$ are divisible by $\mathfrak{a}\mathfrak{g}_1$. It follows that α is not divisible by $\mathfrak{a}\mathfrak{g}_1$. Similarly, it is seen that α is not divisible by any one of the ideals $\mathfrak{a}\mathfrak{g}_2, \mathfrak{a}\mathfrak{g}_3, \cdots, \mathfrak{a}\mathfrak{g}_r$.

ART. 21. LEMMA II. *If* $\mathfrak{a}$, $\mathfrak{b}$ *are two ideals of a realm of rationality* Ω, *such that* $\mathfrak{b} > \mathfrak{a}$, *it is always possible to determine a number* α *that is divisible by* $\mathfrak{a}$ *in such a way that*

$$\mathfrak{a} = \mathfrak{b} + \mathfrak{o}\alpha.$$

For since $\mathfrak{b} > \mathfrak{a}$ and $(\mathfrak{a}, \mathfrak{b}) \neq 0$ there are a finite number of moduls (Vol. I, Art. 142) that are divisors of $\mathfrak{b}$ and multiples of $\mathfrak{a}$. Among these moduls there may be some which are ideals, to which number belong $\mathfrak{a}$ and $\mathfrak{b}$. If such ideals exist, let them be denoted by $\mathfrak{b}_1, \mathfrak{b}_2, \cdots, \mathfrak{b}_r$. We may assume that $\mathfrak{a} \not> \mathfrak{b}$. For, if $\mathfrak{a} > \mathfrak{b}$, then, since $\mathfrak{b} > \mathfrak{a}$, it would follow that $\mathfrak{a} = \mathfrak{b}$, and we would then have at once

$$\mathfrak{a} = \mathfrak{b} + \mathfrak{o}\alpha.$$

If $\mathfrak{a} \not> \mathfrak{b}$, then is $\mathfrak{a}$ divisible by none of the moduls $\mathfrak{b}_1, \mathfrak{b}_2, \cdots, \mathfrak{b}_r$, since these ideals are different and are at the same time multiples of $\mathfrak{a}$ and divisors of $\mathfrak{b}$. Hence, by virtue of the preceding lemma, there is a number α which is divisible by $\mathfrak{a}$ but by none of the $\mathfrak{b}$'s. If next we write

$$\mathfrak{o}\alpha + \mathfrak{b} = \mathfrak{d},$$

then $\mathfrak{d} = \mathfrak{a}$. For, on the one hand, $\mathfrak{a}$ is a common divisor of $\mathfrak{o}\alpha$ and $\mathfrak{b}$, and consequently, $\mathfrak{d} > \mathfrak{a}$. On the other hand, $\mathfrak{d}$ is a divisor of $\mathfrak{b}$ and a multiple of $\mathfrak{a}$. Hence, $\mathfrak{d}$ must be

one of the ideals $\mathfrak{a}, \mathfrak{b}, \mathfrak{b}_1, \mathfrak{b}_2, \cdots, \mathfrak{b}_r$. But $\mathfrak{d}$ is *not* one of the ideals $\mathfrak{b}, \mathfrak{b}_1, \mathfrak{b}_2, \cdots, \mathfrak{b}_r$. For, were $\mathfrak{d} = \mathfrak{b}_3$, say, then since $\mathfrak{o}\alpha > \mathfrak{d}$, it would follow that

$$\mathfrak{o}\alpha > \mathfrak{b}_3,$$

or α is divisible by $\mathfrak{b}_3$, which, owing to the choice of α was excluded. Hence,

$$\mathfrak{d} = \mathfrak{a} \qquad \text{and consequently} \qquad \mathfrak{o}\alpha + \mathfrak{b} = \mathfrak{a}.$$

The following are important consequences of the preceding lemmas:

Every ideal $\mathfrak{a}$ *is either a principal ideal or the greatest common divisor of two principal ideals; and that is, all the numbers of an ideal* $\mathfrak{a}$ *have the form* $\alpha\xi$ *or the form* $\alpha\xi + \beta\eta$, *where* ξ, η *take all the integral values of the realm* Ω.

For, if $\mathfrak{a}$ is *not* a principal ideal, and if β is an arbitrary number divisible by $\mathfrak{a}$, then $\mathfrak{o}\beta$ is not equal to $\mathfrak{a}$. On the other hand $\mathfrak{o}\beta > \mathfrak{a}$. If we put $\mathfrak{o}\beta = \mathfrak{b}$, we have from the lemma a number α divisible by $\mathfrak{a}$, such that

$$\mathfrak{a} = \mathfrak{o}\alpha + \mathfrak{b} = \mathfrak{o}\alpha + \mathfrak{o}\beta.$$

It is to be noted in this expression of an ideal $\mathfrak{a}$ through two principal ideals, that one of the numbers β which produces one of the principal ideals is an *arbitrary* number divisible by $\mathfrak{a}$.

A second important consequence of the lemma is expressed in the formula

$$(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{ac}, \mathfrak{bc}),$$

where $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ are three arbitrary ideals.

In Vol. I, Art. 138, it was seen that if η is an arbitrary number different from zero, then

$$(\eta\mathfrak{a}, \eta\mathfrak{b}) = (\mathfrak{a}, \mathfrak{b}).$$

It follows at once that if $\mathfrak{c}$ is a principal ideal equal to $\mathfrak{o}\eta$, then

$$(\mathfrak{ac}, \mathfrak{bc}) = (\mathfrak{a}, \mathfrak{b}).$$

We may next prove the theorem for the case that $\mathfrak{b} > \mathfrak{a}$, and then later reduce the general case to this special case. If $\mathfrak{b} > \mathfrak{a}$, it has just been seen that a number α which is divisible by $\mathfrak{a}$ may be determined such that

$$\mathfrak{a} = \mathfrak{o}\alpha + \mathfrak{b}.$$

Now, if $\mathfrak{a}$, $\mathfrak{b}$ are two arbitrary ideals and (Art. 10)

$$\mathfrak{d} = \mathfrak{a} + \mathfrak{b}, \qquad \mathfrak{m} = \mathfrak{a} - \mathfrak{b}, \qquad \text{then} \qquad \mathfrak{a}\mathfrak{b} = \mathfrak{m}\mathfrak{d}.$$

It follows that

$$\mathfrak{o}\alpha\mathfrak{b} = (\mathfrak{o}\alpha - \mathfrak{b})(\mathfrak{o}\alpha + \mathfrak{b})$$

or

$$\mathfrak{o}\alpha - \mathfrak{b} = \frac{\mathfrak{o}\alpha\mathfrak{b}}{\mathfrak{o}\alpha + \mathfrak{b}} = \frac{\mathfrak{o}\alpha\mathfrak{b}}{\mathfrak{a}}.$$

We have seen for arbitrary moduls (Vol. I, Art. 137) that

$$(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{a} + \mathfrak{b}, \mathfrak{b}) \qquad \text{and} \qquad (\mathfrak{a}, \mathfrak{b}) = (\mathfrak{a}, \mathfrak{a} - \mathfrak{b}).$$

It follows on the one hand that

$$(\mathfrak{o}\alpha, \mathfrak{b}) = (\mathfrak{o}\alpha + \mathfrak{b}, \mathfrak{b}) = (\mathfrak{a}. \mathfrak{b});$$

and on the other hand that

$$(\mathfrak{o}\alpha, \mathfrak{b}) = (\mathfrak{o}\alpha, \mathfrak{o}\alpha - \mathfrak{b}) = \left(\mathfrak{o}\alpha, \frac{\mathfrak{o}\alpha\mathfrak{b}}{\mathfrak{a}}\right) = \left(\mathfrak{o}, \frac{\mathfrak{b}}{\mathfrak{a}}\right),$$

so that

$$(\mathfrak{a}, \mathfrak{b}) = \left(\mathfrak{o}, \frac{\mathfrak{b}}{\mathfrak{a}}\right).$$

In a similar manner we have

$$(\mathfrak{a}\mathfrak{c}, \mathfrak{b}\mathfrak{c}) = \left(\mathfrak{o}, \frac{\mathfrak{b}\mathfrak{c}}{\mathfrak{a}\mathfrak{c}}\right) = \left(\mathfrak{o}, \frac{\mathfrak{b}}{\mathfrak{a}}\right),$$

and consequently

$$(\mathfrak{a}\mathfrak{c}, \mathfrak{b}\mathfrak{c}) = (\mathfrak{a}, \mathfrak{b}).$$

In general, if $\mathfrak{b}$ is *not* divisible by $\mathfrak{a}$, write

$$\mathfrak{m} = \mathfrak{a} - \mathfrak{b};$$

then, since $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ are ideals,

$$\mathfrak{m}\mathfrak{c} = \mathfrak{a}\mathfrak{c} - \mathfrak{b}\mathfrak{c};$$

and since also $\mathfrak{m} > \mathfrak{a}$, it follows from above that

$$(\mathfrak{a}, \mathfrak{m}) = (\mathfrak{ac}, \mathfrak{mc}) = (\mathfrak{ac}, \mathfrak{ac} - \mathfrak{bc}).$$

On the other hand, we have in the general modul theory

$$(\mathfrak{ac}, \mathfrak{bc}) = (\mathfrak{ac}, \mathfrak{ac} - \mathfrak{bc}),$$

so that

$$(\mathfrak{ac}, \mathfrak{bc}) = (\mathfrak{ac}, \mathfrak{mc}) = (\mathfrak{a}, \mathfrak{m}) = (\mathfrak{a}, \mathfrak{b}).$$

ART. 22. We may now derive the following theorem. *The norm of a product of ideals is equal to the product of the norms of the single factors.*

For (Art. 11)

$$\frac{N(\mathfrak{a})}{N(\mathfrak{b})} = \frac{(\mathfrak{b}, \mathfrak{a})}{(\mathfrak{a}, \mathfrak{b})},$$

where $\mathfrak{a}$, $\mathfrak{b}$ are arbitrary ideals. In a similar manner, it follows that

$$\frac{N(\mathfrak{ab})}{N(\mathfrak{a})} = \frac{(\mathfrak{a}, \mathfrak{ab})}{(\mathfrak{ab}, \mathfrak{a})}.$$

But since

$$(\mathfrak{a}, \mathfrak{ab}) = (\mathfrak{ao}, \mathfrak{ab}) = (\mathfrak{o}, \mathfrak{b})$$

and

$$(\mathfrak{ab}, \mathfrak{a}) = (\mathfrak{ab}, \mathfrak{ao}) = (\mathfrak{b}, \mathfrak{o}),$$

it follows that

$$\frac{N(\mathfrak{ab})}{N(\mathfrak{a})} = \frac{(\mathfrak{o}, \mathfrak{b})}{(\mathfrak{b}, \mathfrak{o})} = N(\mathfrak{b}),$$

so that

$$N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b}).$$

Similarly, it is seen that

$$N(\mathfrak{abc}\cdots) = N(\mathfrak{a})N(\mathfrak{b})N(\mathfrak{c})\cdots.$$

It follows that (Art. 11)

$$N(\mathfrak{a})N(\mathfrak{a}^{-1}) = N(\mathfrak{a}\mathfrak{a}^{-1}) = N(\mathfrak{o}) = 1,$$

or

$$N(\mathfrak{a}^{-1}) = \frac{1}{N(\mathfrak{a})};$$

and also that

$$N\left(\frac{\mathfrak{b}}{\mathfrak{a}}\right) = N(\mathfrak{b}\mathfrak{a}^{-1}) = N(\mathfrak{b})N(\mathfrak{a}^{-1}) = \frac{N(\mathfrak{b})}{N(\mathfrak{a})}.$$

Finally observe that

$$N(\mathfrak{a}^n) = [N(\mathfrak{a})]^n.$$

We know, if α and β are two arbitrary numbers, that

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

In a similar manner, from what we have just seen (Art. 11),

$$N(\mathfrak{a}\beta) = N(\mathfrak{a})N(\mathfrak{o}\beta) = N(\mathfrak{a})\,|N(\beta)|.$$

If we prove the theorem regarding the product of the norms of two arbitrary ideals without using the lemma developed above, we get a real conception of the true meaning of the theorem.

Take first the special case that $\mathfrak{b}$ is a principal ideal. Let

$$\mathfrak{a} = [\alpha_1, \alpha_2, \cdots, \alpha_n], \qquad \mathfrak{o} = [\omega_1, \omega_2, \cdots, \omega_n],$$
$$\mathfrak{b} = \mathfrak{o}\beta = [\omega_1\beta, \omega_2\beta, \cdots, \omega_n\beta],$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\alpha_r = a_{r1}\omega_1 + a_{r2}\omega_2 + \cdots + a_{rn}\omega_n \qquad (r = 1, 2, \cdots, n).$$

The quantities a_{rs} are rational numbers and integral if $\mathfrak{a}$ is an integral ideal. We need not, however, consider $\mathfrak{a}$ integral. Further, let

$$\omega_r\beta = b_{r1}\omega_1 + b_{r2}\omega_2 + \cdots + b_{rn}\omega_n.$$

If we put $|b_{rs}| = B$, it is seen (Art. 11) that

$$|B| = N(\mathfrak{b}) = N(\mathfrak{o}\beta).$$

It is also seen that

$$\mathfrak{a}\beta = [\alpha_1\beta, \alpha_2\beta, \cdots, \alpha_r\beta],$$

and

$$\beta\alpha_r = a_{r1}\beta\omega_1 + a_{r2}\beta\omega_2 + \cdots + a_{rn}\beta\omega_n \qquad (r = 1, 2, \cdots, n)$$
$$= \sum_{t=1}^{t=n}(a_{rt}\beta\omega_t) = \sum_{t,\,s=1}^{n}(a_{rt}b_{ts}\omega_s) = \sum_{\rho=1}^{s=n}c_{rs}\omega_s,$$

where

$$c_{rs} = \sum_{t=1}^{t=n}a_{rt}b_{ts}.$$

It follows that

$$|c_{rs}| = |a_{rt}|\,|b_{ts}|,$$

or

$$N(\mathfrak{a}\beta) = N(\mathfrak{a})N(\beta).$$

The general theorem may be proved as follows. Let α be any number that is divisible by $\mathfrak{a}$ and such that $\frac{\alpha}{\mathfrak{a}}$ is relatively prime to $\mathfrak{a}$. Then if ξ goes through a complete system of $N(\mathfrak{a})$ incongruent numbers (with respect to $\mathfrak{a}$), while η goes through a complete system of $N(\mathfrak{b})$ incongruent (with respect to $\mathfrak{b}$) integers, it is evident that the expression $\alpha\eta+\xi$ presents a complete system of incongruent integers (with respect to $\mathfrak{a}\mathfrak{b}$).

For, observe that

$$\alpha\eta+\xi \not\equiv \alpha\eta_1+\xi_1 \pmod{\mathfrak{a}\mathfrak{b}}. \tag{1}$$

For if $\xi \not\equiv \xi_1$, then (1) is not divisible by $\mathfrak{a}$; and if $\xi = \xi_1$, then (1) is not divisible by $\mathfrak{a}\mathfrak{b}$ unless $\eta \equiv \eta_1 \pmod{\mathfrak{b}}$. Such a system, therefore, contains $N(\mathfrak{a})N(\mathfrak{b})$ incongruent numbers (mod. $\mathfrak{a}\mathfrak{b}$), and that is

$$N(\mathfrak{a})N(\mathfrak{b}) = N(\mathfrak{a}\mathfrak{b}).$$

ART. 23. THEOREM. *If $\mathfrak{a}$ is an ideal and if g is an arbitrary rational integer, a number α that is divisible by $\mathfrak{a}$ may always be determined such that $(\mathfrak{a}, \mathfrak{o}\alpha)$ is relatively prime to g.*

For $g\mathfrak{a}$ is divisible by $\mathfrak{a}$, and consequently (Art. 21) we may determine a number α divisible by $\mathfrak{a}$, such that

$$\mathfrak{a} = \mathfrak{o}\alpha + g\mathfrak{a}.$$

Further, since $\mathfrak{o}\alpha > \mathfrak{a}$, it follows that $\frac{\mathfrak{o}\alpha}{\mathfrak{a}}$ is an integral ideal equal to $\mathfrak{f}$, say; or, $\mathfrak{o}\alpha = \mathfrak{a}\mathfrak{f}$. It follows that

$$\mathfrak{a} = \mathfrak{a}\mathfrak{o} = \mathfrak{o}\alpha + g\mathfrak{a} \qquad \text{or} \qquad \mathfrak{a}\mathfrak{o} = \mathfrak{a}\mathfrak{f} + \mathfrak{a}g\mathfrak{o}.$$

We then have

$$\mathfrak{a}^{-1}\mathfrak{a}\mathfrak{o} = \mathfrak{a}^{-1}\mathfrak{a}\mathfrak{f} + \mathfrak{a}^{-1}\mathfrak{a}g\mathfrak{o}, \qquad \text{or} \qquad \mathfrak{o} = \mathfrak{f} + g\mathfrak{o}.$$

It is thus seen that g is relatively prime to $\mathfrak{f}$ and conse-

quently (Art. 19) to

$$N(\mathfrak{f}) = \frac{(\mathfrak{o}, \mathfrak{f})}{(\mathfrak{f}, \mathfrak{o})} = (\mathfrak{o}, \mathfrak{f}) = (\mathfrak{o}\mathfrak{a}, \mathfrak{f}\mathfrak{a}) = (\mathfrak{o}\mathfrak{a}, \mathfrak{o}\alpha) = (\mathfrak{a}, \mathfrak{o}\alpha).$$

We had in general (Art. 11)

$$\frac{(\mathfrak{a}, \mathfrak{b})}{(\mathfrak{b}, \mathfrak{a})} = \frac{N(\mathfrak{b})}{N(\mathfrak{a})}.$$

It follows here that

$$\frac{(\mathfrak{a}, \mathfrak{o}\alpha)}{(\mathfrak{o}\alpha, \mathfrak{a})} = \frac{N(\mathfrak{o}\alpha)}{N(\mathfrak{a})} = \frac{|N(\alpha)|}{N(\mathfrak{a})};$$

or, since $\mathfrak{o}\alpha > \mathfrak{a}$, this formula becomes

$$(\mathfrak{a}, \mathfrak{o}\alpha) = \frac{|N(\alpha)|}{N(\mathfrak{a})}.$$

Hence $N(\alpha)$ is divisible by $N(\mathfrak{a})$; and as just seen, a number α divisible by $\mathfrak{a}$ may be so determined that $\frac{|N(\alpha)|}{N(\mathfrak{a})}$ is relatively prime to a given rational integer g.

From this it may be proved that $N(\mathfrak{a})$ *is the greatest common divisor of all numbers* $N(\alpha)$, *where* α *takes all values that are divisible by* $\mathfrak{a}$.

For, if β is an arbitrary number divisible by $\mathfrak{a}$, and if we put $g = (\mathfrak{a}, \mathfrak{o}\beta)$, then a number α divisible by $\mathfrak{a}$ may be determined, such that $(\mathfrak{a}, \mathfrak{o}\alpha)$ is relatively prime to $g = (\mathfrak{a}, \mathfrak{o}\beta)$. But since

$$(\mathfrak{a}, \mathfrak{o}\alpha) = \frac{|N(\alpha)|}{N(\mathfrak{a})} \qquad \text{and} \qquad (\mathfrak{a}, \mathfrak{o}\beta) = \frac{|N(\beta)|}{N(\mathfrak{a})},$$

and since $(\mathfrak{a}, \mathfrak{o}\alpha)$ and $(\mathfrak{a}, \mathfrak{o}\beta)$ are relatively prime, it is seen that $N(\mathfrak{a})$ is the greatest common divisor of $|N(\alpha)|$ and $|N(\beta)|$.

It follows further that $\mathfrak{a}$ is the greatest common divisor of $\mathfrak{o}\alpha$ and $\mathfrak{o}\beta$. For, write

$$\mathfrak{o}\alpha + \mathfrak{o}\beta = \mathfrak{d}.$$

Then, since $\mathfrak{a}$ is a common divisor of $\mathfrak{o}\alpha$ and $\mathfrak{o}\beta$, it is clear

that $\frac{\mathfrak{d}}{\mathfrak{a}}$ is an integral ideal, say, $\mathfrak{b}$. We thus have

$$\mathfrak{d} = \mathfrak{a}\mathfrak{b}.$$

Hence, as $\mathfrak{o}\alpha > \mathfrak{d}$, or by $\mathfrak{a}\mathfrak{b}$, and as $\mathfrak{o}\beta > \mathfrak{d}$, or by $\mathfrak{a}\mathfrak{b}$, it follows that $N(\mathfrak{o}\alpha)$ or $|N(\alpha)|$ as well as $N(\mathfrak{o}\beta)$ or $|N(\beta)|$ is divisible by $N(\mathfrak{a}\mathfrak{b})$ and consequently by $N(\mathfrak{a})N(\mathfrak{b})$ so that $N(\mathfrak{b}) = 1$. It is thus seen that $\mathfrak{b} = \mathfrak{o}$, and from above

$$\mathfrak{o}\alpha + \mathfrak{o}\beta = \mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{o} = \mathfrak{a}.$$

Compare this result with the theorem in Art. 21.

ART. **24.** Let $\mathfrak{a}$ be an integral ideal denoted by $(\alpha_1, \alpha_2, \cdots, \alpha_n)$, in which the basal elements (Art. 12) have been so chosen that every integer α that is divisible by $\mathfrak{a}$ has the form

$$\alpha = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n,$$

where the x's are rational integers. If we denote conjugate quantities by upper indices and put $\alpha = \alpha^{(1)}$, it is seen that

$$N(\alpha) = \prod_{s=1}^{s=n} (\alpha^{(s)}) = \prod_{s=1}^{s=n} (\alpha_1^{(s)} x_1 + \alpha_2^{(s)} x_2 + \cdots + \alpha_n^{(s)} x_n).$$

It is asserted that: *There is an integral homogeneous form X of the quantities $x_1, x_2, \cdots, x_n$ with rational integral coefficients, such that*

$$N(\alpha) = N(\mathfrak{a})X.$$

For, let

$$\mathfrak{o} = [\omega_1, \omega_2, \cdots, \omega_n]$$

and note, since $\mathfrak{a}$ is an ideal, that $\mathfrak{o}\mathfrak{a} > \mathfrak{a}$. It follows that $\omega_r \alpha_s (r = 1, 2, \cdots, n)$ is divisible by $\mathfrak{a}$. Consequently,

$$\omega_r \alpha_s = p_{1r}^{(s)} \alpha_1 + p_{2r}^{(s)} \alpha_2 + \cdots + p_{nr}^{(s)} \alpha_n = \sum_{\nu=1}^{\nu=n} p_{\nu r}^{(s)} \alpha_\nu,$$

where $p_{\nu r}^{(s)}$ are rational integers. Hence, also

$$\sum_{s=1}^{s=n} \omega_r \alpha_s x_s = \alpha_1 \sum_{s=1}^{s=n} p_{1r}^{(s)} x_s + \alpha_2 \sum_{s=1}^{s=n} p_{2r}^{(s)} x_s + \cdots + \alpha_n \sum_{s=1}^{s=n} p_{nr}^{(s)} x_s$$

$$= \alpha_1 x_{r1} + \alpha_2 x_{r2} + \cdots + \alpha_n x_{rn},$$

where

$$x_{rs} = p_{sr}^{(1)}x_1 + p_{sr}^{(2)}x_2 + \cdots + p_{sr}^{(n)}x_n \quad (s=1, 2, \cdots, n;\ r=1, 2, \cdots, n).$$

Since $\mathfrak{a}$ is an integral ideal, we have

$$\alpha_t = \sum_{\nu=1}^{\nu=n} a_{t\nu}\omega_\nu,$$

where $a_{t\nu}$ are rational integers; and also (Vol. I, Art. 150)

$$N(\mathfrak{a}) = (\mathfrak{o}, \mathfrak{a}) = |a_{t\nu}|.$$

It is also seen that

$$\omega_r\alpha = \omega_r\alpha_1x_1 + \omega_r\alpha_2x_2 + \cdots + \omega_r\alpha_nx_n = \sum_{s=1}^{s=n} \omega_r\alpha_sx_s$$

$$= \sum_{t=1}^{t=n} x_{rt}\alpha_t = \sum_{s,\,t=1}^{n} x_{rt}a_{ts}\omega_s$$

$$= \omega_1 \sum_{t=1}^{t=n} x_{rt}a_{t1} + \omega_2 \sum_{t=1}^{t=n} x_{rt}a_{t2} + \cdots + \omega_r \sum_{t=1}^{t=n} x_{rt}a_{tn};$$

or

$$\omega_r\alpha = \omega_1y_{r1} + \omega_2y_{r2} + \cdots + \omega_ny_{rn},$$

where

$$y_{rs} = \sum_{t=1}^{t=n} x_{rt}a_{ts} \quad (r=1, 2, \cdots, n;\ s=1, 2, \cdots, n).$$

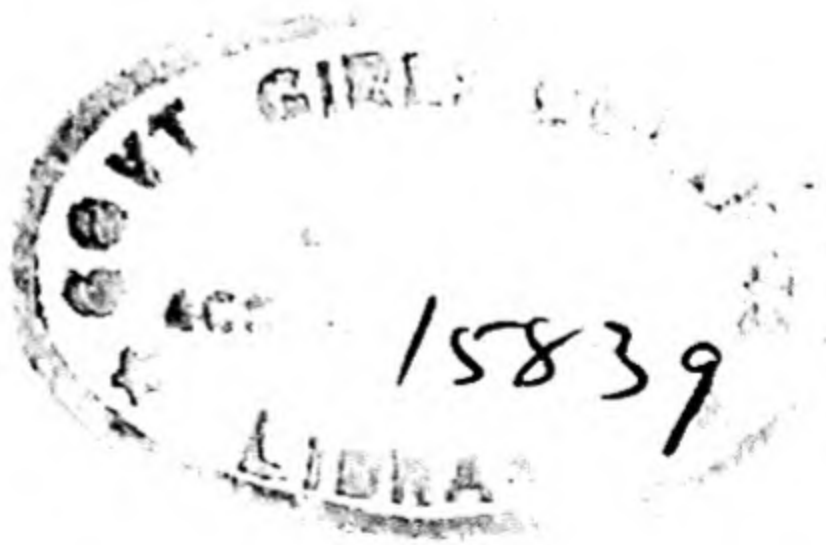
Hence, (Art. 11)

$$N(\mathfrak{o}\alpha) = N(\alpha) = |y_{rs}| = |a_{ts}| \cdot |x_{rt}| = N(\mathfrak{a})\,|x_{rt}| = N(\mathfrak{a})X.$$

The n^2 quantities x_{rs} are linear homogeneous functions of $x_1, x_2, \cdots, x_n$ with rational integral coefficients, so that the determinant $X = |x_{rt}|$ is a function of the nth degree in $x_1, x_2, \cdots, x_n$ with rational integral coefficients. The value of X is $\dfrac{N(\alpha)}{N(\mathfrak{a})} = (\mathfrak{a}, \mathfrak{o}\alpha)$; and if for α we write all numbers that are divisible by $\mathfrak{a}$, we have all values of X expressed through $(\mathfrak{a}, \mathfrak{o}\alpha)$. Since (Art. 23) we may give to the variables in X such values that the value of X thus had is relatively prime to a fixed integer g, it follows that the coefficients of X have no greatest common divisor other than unity. Such a form is called a

primitive form. It is seen then that all the values that X can take do not have a greatest common divisor other than unity.

Since the ideal $\mathfrak{a}$ has an infinitude of such bases $(\alpha_1, \alpha_2, \cdots, \alpha_n)$, there corresponds to it a *class* of infinitely many equivalent forms X, which may be transformed into one another through linear substitutions with integral rational coefficients. Observe also that the same forms may be derived from every ideal that is equivalent to $\mathfrak{a}$. Hence to every ideal class there corresponds a class of forms. The multiplication of the ideals and the ideal classes leads to the composition of the forms and classes of forms. (See Dedekind, *Werke*, Vol. I, p. 119.) This offers another approach to the Kronecker Theory as outlined in Chapter IV. Chapter XI on "Composite Forms" admits wide extensions along these lines. Note also Chapter XII of Vol. I, which was given in great detail as an introduction to what may be done in this general theory.


GOVT GIRL
15839
LIBRA

CHAPTER III

PRIME IDEALS

ART. 25. The following discussion will be confined to integral ideals, and when the term *ideal* is used, an *integral ideal* is to be understood. The norm of an integral ideal $\mathfrak{a}$, that is, of an ideal which consists only of algebraic integers of the realm Ω, or which, in other words, is divisible by $\mathfrak{o}$, is

$$N(\mathfrak{a}) = (\mathfrak{o}, \mathfrak{a}),$$

and is always different from zero (Art. 16). The norm of an ideal is only equal to 1, if $\mathfrak{a} = \mathfrak{o}$, since then, and only then, is $(\mathfrak{o}, \mathfrak{a}) = 1$.

The following theorem may be proved: *An ideal* $\mathfrak{a} = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ *is divisible only by a finite number of ideals* $\mathfrak{b}_k = (\beta_{1k}, \beta_{2k}, \cdots, \beta_{nk})$ $(k = 1, 2, \cdots)$.

For, if $\mathfrak{a}$ is divisible by $\mathfrak{b}_k$, every number α of $\mathfrak{a}$ is divisible by $\mathfrak{b}_k$. Hence $N(\alpha)$ being a rational integer, say g, of $\mathfrak{a}$ is congruent to zero (mod. $\mathfrak{b}_k$). Hence all the $\mathfrak{b}$'s contain g as an element. Observe next that the basal elements β of the $\mathfrak{b}$'s, being integers in Ω, are of the form

$$\beta_{ih} = b_{1h}\omega_1 + b_{2h}\omega_2 + \cdots + b_{nh}\omega_n \quad (h = 1, 2, \cdots, n),$$

where the b's are rational integers. Further, the b's may be reduced (mod. g) with the result that there are only a finite number of different ideals $\mathfrak{b}_k$.

If $\mathfrak{a}$ and $\mathfrak{b}$ are two arbitrary moduls such that

$$\mathfrak{b} > \mathfrak{a} \qquad \text{and} \qquad (\mathfrak{a}, \mathfrak{b}) \neq 0,$$

there are (Vol. I, Art. 142) only a finite number of moduls $\mathfrak{r}$ which have the property that $\mathfrak{b} > \mathfrak{r} > \mathfrak{a}$. Hence, if $\mathfrak{a}$ is an

integral ideal, in which case

$$\mathfrak{a} > \mathfrak{o} \qquad \text{and} \qquad (\mathfrak{o}, \mathfrak{a}) \neq 0,$$

there are only a finite number of integral ideals $\mathfrak{i}$ which are at the same time divisors of $\mathfrak{a}$ and multiples of $\mathfrak{o}$, say

$$\mathfrak{a} > \mathfrak{b}_k > \mathfrak{b}_{k-1} > \mathfrak{b}_{k-2} > \cdots > \mathfrak{b}_2 > \mathfrak{b}_1 > \mathfrak{o}.$$

From this it is evident that no $\mathfrak{b}$ can occur to an infinite power as a divisor of $\mathfrak{a}$.

ART. **26. Prime Ideal.** If an ideal $\mathfrak{a}$ has the property that it has besides $\mathfrak{o}$ and $\mathfrak{a}$ no other divisors, it is said to be a *prime* ideal. If $\mathfrak{a}$ has *not* this property, it is called a *composite* ideal. The existence of a prime ideal is proved below.

Let $\mathfrak{p}$ be a prime ideal, and let $\mathfrak{a}$ be an arbitrary ideal. Two cases are possible. Either $\mathfrak{a}$ is divisible by $\mathfrak{p}$; or $\mathfrak{a}$ and $\mathfrak{p}$ are relatively prime. For, if $\mathfrak{d} = \mathfrak{a} + \mathfrak{p}$, then is $\mathfrak{p}$ divisible by $\mathfrak{d}$; and $\mathfrak{d}$ is either equal to $\mathfrak{p}$ or to $\mathfrak{o}$. If $\mathfrak{d} = \mathfrak{p}$, then is $\mathfrak{a}$ divisible by $\mathfrak{p}$; and if $\mathfrak{d} = \mathfrak{o}$, then is $\mathfrak{p} + \mathfrak{a} = \mathfrak{o}$, in which case $\mathfrak{a}$ and $\mathfrak{p}$ are relatively prime.

THEOREM. *If a product of several factors is divisible by a prime ideal* $\mathfrak{p}$, *one of the factors is divisible by* $\mathfrak{p}$; *or, if none of the ideals* $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \cdots$ *is divisible by* $\mathfrak{p}$, *then also the product* $\mathfrak{abc}\cdots$ *is not divisible by* $\mathfrak{p}$. This theorem is known as the *Fundamental Theorem.*

For, if $\mathfrak{p}$ is relatively prime to $\mathfrak{a}$, to $\mathfrak{b}$, to $\mathfrak{c}$, to $\cdots$, which must be the case if none of these ideals is divisible by $\mathfrak{p}$, then (Art. 17) is $\mathfrak{p}$ relatively prime to $\mathfrak{abc}\cdots$; and consequently $\mathfrak{abc}\cdots$ is *not* divisible by $\mathfrak{p}$.

The following theorem offers a proof of the existence of prime ideals. *Every integral ideal which is different from* $\mathfrak{o}$ *is either itself a prime ideal or is divisible by a prime ideal.*

For, if $\mathfrak{a}$ is not a prime ideal, it has a divisor $\mathfrak{a}_1$, which is different from $\mathfrak{o}$. Two cases are possible: either $\mathfrak{a}_1$ is a prime ideal, in which case the theorem is proved; or, $\mathfrak{a}_1$ is

not a prime ideal. In the latter case $\mathfrak{a}_1$ is divisible by an ideal $\mathfrak{a}_2$, which is different from $\mathfrak{o}$, and here again two cases are possible: either $\mathfrak{a}_2$ is a prime ideal, in which case the assertion is proved, since $\mathfrak{a} > \mathfrak{a}_1 > \mathfrak{a}_2$; or, $\mathfrak{a}_2$ is *not* a prime ideal, etc. We must finally reach an ideal, which is a prime ideal. Thus we have $\mathfrak{a} > \mathfrak{a}_1 > \mathfrak{a}_2 > \mathfrak{a}_3 > \cdots$, and the ideals $\mathfrak{a}_1, \mathfrak{a}_2, \cdots$ are all different. For, if $\mathfrak{a}_r = \mathfrak{a}_s (s > r)$, then also $\mathfrak{a}_{r+1} = \mathfrak{a}_r = \mathfrak{a}_s$. On the one hand $\mathfrak{a}_{r+1} > \mathfrak{a}_{r+2} > \cdots > \mathfrak{a}_s$ and on the other hand $\mathfrak{a}_s > \mathfrak{a}_r > \mathfrak{a}_{r+1} > \mathfrak{a}_{r+2}$. Hence $\mathfrak{a}_{r+1} = \mathfrak{a}_r$, which is contrary to the hypothesis. Further, since the number of ideals $\mathfrak{a}_1, \mathfrak{a}_2, \cdots$ is finite, there must occur in the above process the case where a prime ideal is reached. It is thus proved that every ideal different from $\mathfrak{o}$ is either a prime ideal or is divisible by a prime ideal. From this it is also seen that there exist prime ideals. The theorem may be proved also by the consideration of the norms.

The unit ideal $\mathfrak{o}$ is *not* considered a prime ideal.

ART. 27. THEOREM. *Every ideal which is different from* $\mathfrak{o}$ *may be decomposed into a product of prime ideals and this decomposition is unique.*

For, if $\mathfrak{a} \neq \mathfrak{o}$, then is $\mathfrak{a}$ divisible by a prime ideal $\mathfrak{p}_1$, so that

$$\frac{\mathfrak{a}}{\mathfrak{p}_1} = \mathfrak{a}_1 \qquad \text{or} \qquad \mathfrak{a} = \mathfrak{p}_1 \mathfrak{a}_1,$$

where $\mathfrak{a}_1$ is an integral ideal. If $\mathfrak{a}_1 \neq \mathfrak{o}$, then is $\mathfrak{a}_1$ divisible by a prime ideal $\mathfrak{p}_2$, so that $\mathfrak{a}_1 = \mathfrak{p}_2 \mathfrak{a}_2$, where $\mathfrak{a}_2$ is an integral ideal, and then $\mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{a}_2$.

We must finally have $\mathfrak{a}_r = \mathfrak{o}$; for $\mathfrak{a} > \mathfrak{a}_1 > \mathfrak{a}_2 > \cdots$, where the ideals $\mathfrak{a}, \mathfrak{a}_1, \mathfrak{a}_2, \cdots$ are all different, and as an ideal can have only a finite number of divisors, we must have finally $\mathfrak{a}_r = \mathfrak{o}$, and consequently

$$\mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r.$$

The prime ideals are not necessarily all different. It is further asserted that this decomposition of $\mathfrak{a}$ into its prime factors is unique; that is, if $\mathfrak{a} = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_m$, where $\mathfrak{q}_1$, $\mathfrak{q}_2$, $\cdots$, $\mathfrak{q}_m$ are prime ideals, then is $m = r$; and the prime ideals $\mathfrak{q}_1$, $\mathfrak{q}_2$, $\cdots$, $\mathfrak{q}_m$ are, neglecting the sequence, the same as the prime ideals $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\cdots$, $\mathfrak{p}_r$. For $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r$ is divisible by the prime ideal $\mathfrak{q}_1$. Hence, one of the prime ideals $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\cdots$, $\mathfrak{p}_r$ must be divisible by $\mathfrak{q}_1$, say, $\mathfrak{p}_s$. But the prime ideal $\mathfrak{p}_s$ has only the divisors $\mathfrak{o}$ and $\mathfrak{p}_s$. Further, $\mathfrak{q}_1 \neq \mathfrak{o}$, since $\mathfrak{q}_1$ is a prime ideal. Hence we must have $\mathfrak{q}_1 = \mathfrak{p}_s$ and, since

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_m,$$

it follows that

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_s\mathfrak{p}_s^{-1} \cdots \mathfrak{p}_r = \mathfrak{p}_s^{-1}\mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_m,$$

or

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_{s-1}\mathfrak{p}_{s+1} \cdots \mathfrak{p}_r = \mathfrak{q}_2\mathfrak{q}_3 \cdots \mathfrak{q}_m.$$

It is also seen that one of the ideals $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\cdots$, $\mathfrak{p}_{s-1}$, $\mathfrak{p}_{s+1}$, $\cdots$, $\mathfrak{p}_r$ is divisible by $\mathfrak{q}_2$, etc. It follows that the prime ideals $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\cdots$, $\mathfrak{p}_r$ are, neglecting the sequence, identical with the ideals $\mathfrak{q}_1$, $\mathfrak{q}_2$, $\cdots$, $\mathfrak{q}_m$ and at the same time $r = m$. It follows also that the decomposition of an integral ideal into its prime factors is possible in only one way.

If in the product of prime ideals equal ideals are united, it is seen that any ideal may be written

$$\mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_r^{e_r},$$

where the rational integers e_1, e_2, $\cdots$, e_r are all greater than or equal to unity.

If $\mathfrak{d}$ is a divisor of $\mathfrak{a}$, so that $\frac{\mathfrak{a}}{\mathfrak{d}} = \mathfrak{c}$, where $\mathfrak{c}$ is an integral ideal, then is

$$\mathfrak{c} = \mathfrak{p}_1^{s_1}\mathfrak{p}_2^{s_2} \cdots \mathfrak{p}_r^{s_r}; \qquad \mathfrak{d} = \mathfrak{p}_1^{t_1}\mathfrak{p}_2^{t_2} \cdots \mathfrak{p}_r^{t_r},$$

where s_1, s_2, $\cdots$, s_r, t_1, t_2, $\cdots$, t_r are rational integers

including zero. Hence, we have

$$\mathfrak{c}\mathfrak{d} = \mathfrak{p}_1^{s_1+t_1}\mathfrak{p}_2^{s_2+t_2}\cdots\mathfrak{p}_r^{s_r+t_r} = \mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r}.$$

As an ideal may be decomposed into a product of prime ideals in only one way, it is evident that

$$s_k + t_k = e_k \qquad (k=1, 2, \cdots, r).$$

Reciprocally, if $\mathfrak{d}$ has the form $\mathfrak{p}_1^{t_1}\cdots\mathfrak{p}_r^{t_r}$, where t_i is one of the numbers $0, 1, 2, \cdots, e_k$ $(k=1, 2, \cdots, r)$, then $\mathfrak{d}$ is a divisor of $\mathfrak{a}$. For, in that case

$$\frac{\mathfrak{a}}{\mathfrak{d}} = \mathfrak{p}_1^{e_1-t_1}\mathfrak{p}_2^{e_2-t_2}\cdots\mathfrak{p}_r^{e_r-t_r},$$

which is an integral ideal.

It is further seen that all divisors of $\mathfrak{a}$ are had, if in

$$\mathfrak{d} = \mathfrak{p}_1^{t_1}\mathfrak{p}_2^{t_2}\cdots\mathfrak{p}_r^{t_r}$$

t_1 takes all the values $0, 1, \cdots, e_1$; if t_2 takes all the values $0, 1, \cdots, e_2$; $\cdots$; if t_r takes all the values $0, 1, \cdots, e_r$; and consequently, the number of all the divisors of $\mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r}$ is $(e_1+1)(e_2+1)\cdots(e_r+1)$.

From what precedes it is evident that all the theorems relative to prime numbers in the theory of natural numbers, may be applied at once to the theory of prime ideals. It is consequently unnecessary to go further in this theory.

The following theorems may be mentioned: If

$$\mathfrak{a} = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\cdots\mathfrak{p}_r^{a_r}, \qquad \mathfrak{b} = \mathfrak{p}_1^{b_1}\mathfrak{p}_2^{b_2}\cdots\mathfrak{p}_r^{b_r},$$

where $a_1, a_2, \cdots, a_r; b_1, b_2, \cdots, b_r$ are all positive integers including zero, and if m_k is the greater, while d_k is the smaller of the two numbers, a_k and b_k $(k=1, 2, \cdots, r)$, we have

$$\mathfrak{a}+\mathfrak{b} = \mathfrak{d} = \mathfrak{p}_1^{d_1}\mathfrak{p}_2^{d_2}\cdots\mathfrak{p}_r^{d_r},$$

and

$$\mathfrak{a}-\mathfrak{b} = \mathfrak{m} = \mathfrak{p}_1^{m_1}\mathfrak{p}_2^{m_2}\cdots\mathfrak{p}_r^{m_r}.$$

ART. 28. **The Fundamental Ideal.** If $\mathfrak{a}$ is an arbitrary modul, the complementary modul (Vol. I, Art. 171) was

represented by $\mathfrak{a}'$. It was proved that

$$(\mathfrak{ab})' = \frac{\mathfrak{a}'}{\mathfrak{b}} = \frac{\mathfrak{b}'}{\mathfrak{a}},$$

where $\mathfrak{b}$ was an arbitrary finite modul. If then we put $\mathfrak{b} = \mathfrak{a}'$, it is seen that

$$(\mathfrak{aa}')' = \frac{\mathfrak{a}'}{\mathfrak{a}'} = \frac{\mathfrak{a}}{\mathfrak{a}}.$$

Further, if $\mathfrak{a}$ is an ideal,

$$\frac{\mathfrak{a}'}{\mathfrak{a}'} = \frac{\mathfrak{a}}{\mathfrak{a}} = \mathfrak{o}.$$

From this it follows at once that $\mathfrak{a}'$ is an ideal, and we now define $\mathfrak{a}$ and $\mathfrak{a}'$ as expressed above, as complementary moduls (ideals).

Since

$$(\mathfrak{aa}')' = \mathfrak{o},$$

it follows that

$$\mathfrak{aa}' = \mathfrak{o}',$$

where $\mathfrak{o}'$ is the complementary ideal of $\mathfrak{o}$. Writing

$$\mathfrak{o} = [\omega_1, \omega_2, \cdots, \omega_n],$$
$$\mathfrak{o}' = [\omega_1', \omega_2', \cdots, \omega_n'],$$

we proved (Vol. I, Art. 171) that, if α is any number of the fixed realm Ω,

$$\alpha = \sum_{s=1}^{s=n} \{S(\alpha\omega_s)\omega_s'\},$$

and consequently also

$$\omega_r = \sum_{s=1}^{s=n} \{S(\omega_r\omega_s)\omega_s'\} \qquad (r = 1, 2, \cdots, n).$$

The quantities $\omega_r\omega_s (r, s = 1, 2, \cdots, n)$ being algebraic integers in Ω, their spurs are rational integers.

It follows that $\omega_1, \omega_2, \cdots, \omega_n$ may be expressed linearly through $\omega_1', \omega_2', \cdots, \omega_n'$ with rational integral coefficients. Hence also $\mathfrak{o}$ is divisible by $\mathfrak{o}'$, and $(\mathfrak{o}, \mathfrak{o}') = 1$. It is then

seen (Vol. I, Art. 153) that the absolute value of the determinant is

$$|S(\omega_r\omega_s)| = \frac{(\mathfrak{o}', \mathfrak{o})}{(\mathfrak{o}, \mathfrak{o}')} = (\mathfrak{o}', \mathfrak{o}),$$

so that the basal invariant D is

$$D = (\mathfrak{o}', \mathfrak{o}).$$

Since $\mathfrak{o}$ is divisible by $\mathfrak{o}'$, it follows that $\frac{\mathfrak{o}}{\mathfrak{o}'}$ is an integral ideal equal to $\mathfrak{d}$, say, or

$$\mathfrak{d} = \mathfrak{o}'^{-1} \qquad \text{or} \qquad \mathfrak{o}' = \mathfrak{d}^{-1}.$$

It is seen that $\mathfrak{d}$ is the reciprocal of the ideal $\mathfrak{o}'$, where $\mathfrak{o}'$ is the complementary ideal of $\mathfrak{o}$.

The ideal $\mathfrak{d}$ is called the *basal* or *fundamental* [1] ideal (*Grundideal*).

The norm of the basal ideal is in absolute value equal to the basal invariant D. For, from above (Art. 11)

$$|D| = (\mathfrak{o}', \mathfrak{o}) = (\mathfrak{o}'\mathfrak{d}, \mathfrak{o}\mathfrak{d}) = (\mathfrak{o}, \mathfrak{d}) = N(\mathfrak{d}).$$

Further, since

$$\mathfrak{a}\mathfrak{a}' = \mathfrak{o}',$$

it is seen that

$$\mathfrak{a}' = \mathfrak{a}^{-1}\mathfrak{d}^{-1} = (\mathfrak{a}\mathfrak{d})^{-1}.$$

From this it is evident that a theory of complementary ideals is superfluous, for as soon as the basal ideal $\mathfrak{d}$ has been found, the ideal $\mathfrak{a}'$, which is complementary to $\mathfrak{a}$, is known from the formula just written.

ART. 29. **The Degree of a Prime Ideal.** Let $\mathfrak{p}$ be a prime ideal, and let p be the smallest rational integer divisible by $\mathfrak{p}$. It was seen (Vol. I, Art. 170) that all other rational integers that are divisible by $\mathfrak{p}$ are integral multiples of p.

It is asserted that p *is a rational prime integer.* An indirect proof of this assertion is given here. Suppose

[1] See also Art. 106; and Dedekind, *Werke*, Vol. I, p. 381.

that p is a product of two rational integers r and s. Then rs is divisible by $\mathfrak{p}$, and consequently

$$\mathfrak{o}r \cdot \mathfrak{o}s > \mathfrak{p}.$$

Hence, since $\mathfrak{p}$ is a prime ideal, either $\mathfrak{o}r$ or $\mathfrak{o}s$ is divisible by $\mathfrak{p}$, and consequently r or s is divisible by $\mathfrak{p}$. But if r is divisible by $\mathfrak{p}$, we have just seen that r is divisible by p, so that $r=p$ and $s=1$.

The above result may be stated as follows: *All rational integers that are divisible by a prime ideal* $\mathfrak{p}$ *are multiples of a definite prime rational integer* p, *where* p *is the smallest rational integer that is divisible by* $\mathfrak{p}$.

If p is the prime integer, which is the smallest rational integer divisible by the prime ideal $\mathfrak{p}$, then is $\mathfrak{o}p > \mathfrak{p}$, so that $N(\mathfrak{o}p)$ or p^n is divisible by $N(\mathfrak{p})$. It follows that $N(\mathfrak{p})$ is a definite power of p, say, p^f. The number f is called the *degree* of the prime ideal $\mathfrak{p}$.

The prime rational integer may be factored into its prime ideal factors, say in the form

$$\mathfrak{o}p = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_r^{e_r}.$$

Accordingly, p is divisible by each of the r prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_r$. Since p is a prime integer, it follows from above that p is the smallest rational integer which is divisible by $\mathfrak{p}_\nu (\nu = 1, 2, \cdots, r)$; and further, if f_ν is the degree of $\mathfrak{p}_\nu$, so that

$$N(\mathfrak{p}_\nu) = p^{f_\nu} \qquad (\nu = 1, 2, \cdots, r),$$

it follows that

$$N(\mathfrak{o}p) = p^n = p^{e_1 f_1} p^{e_2 f_2} \cdots p^{e_r f_r}.$$

We thus have

$$n = e_1 f_1 + e_2 f_2 + \cdots + e_r f_r.$$

The integers $e_1, e_2, \cdots, e_r$ are as a rule all equal to unity. It will be seen below that only when p is a divisor of the basal invariant D, is $\mathfrak{o}p$ divisible by a prime ideal raised to the second or higher power.

ART. 30. THEOREM. *If one of the above integers* $e_1, e_2, \cdots, e_r$ *is greater than unity, so that* $\mathfrak{o}p$ *is divisible by the square of a prime ideal, then the discriminant* D *is always divisible by* p.

In the proof of this theorem it is necessary to introduce a lemma which will be used often in the sequel.

LEMMA. *If* $R(\alpha, \beta, \gamma, \cdots)$ *is an integral function of* $\alpha, \beta, \gamma, \cdots$ *with rational integral coefficients, and if* p *is a rational prime integer*, then is

$$[R(\alpha, \beta, \gamma, \cdots)]^p \equiv R(\alpha^p, \beta^p, \gamma^p, \cdots) \pmod{p}.$$

For the function $R(\alpha, \beta, \gamma, \cdots)$ consists of a sum of terms of the form

$$l\alpha^a\beta^b\gamma^c\cdots + l'\alpha^{a'}\beta^{b'}\gamma^{c'}\cdots + \cdots.$$

If this expression is raised to the pth power by the polynomial theorem, the coefficients that occur are of the form $\frac{p!}{r!s!t!\cdots}$, where $r, s, t, \cdots$ take all possible combinations of positive integral values, including zero, which satisfy the equation

$$r+s+t+\cdots = p.$$

It is clear that none of the numbers $r, s, t, \cdots$ is greater than p. If one of these numbers is equal to p, the others are all zero. In all other cases, the coefficients are divisible by p; for it is proved in the Theory of Combinations, that these coefficients are integral. It follows that

$$[l\alpha^a\beta^b\gamma^c\cdots + l'\alpha^{a'}\beta^{b'}\gamma^{c'}\cdots + \cdots]^p \equiv l^p(\alpha^p)^a(\beta^p)^b(\gamma^p)^c\cdots + l'^p(\alpha^p)^{a'}(\beta^p)^{b'}(\gamma^p)^{c'}\cdots + \cdots \pmod{p}.$$

But from Fermat's Theorem it follows that

$$l^p \equiv l \pmod{p}, \qquad l'^p \equiv l' \pmod{p}, \cdots,$$

and consequently,

$$R(\alpha, \beta, \gamma, \cdots)^p \equiv l(\alpha^p)^a(\beta^p)^b(\gamma^p)^c \cdots + l'(\alpha^p)^{a'}(\beta^p)^{b'}(\gamma^p)^{c'} \cdots + \cdots \pmod{p},$$

or

$$\{R(\alpha, \beta, \gamma, \cdots)\}^p \equiv R(\alpha^p, \beta^p, \gamma^p, \cdots) \pmod{p}.$$

ART. 31. Returning to the theorem stated at the beginning of the preceding article, suppose that

$$\mathfrak{o}p = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_r^{e_r},$$

where one of the integers $e_1, e_2, \cdots, e_r$ is greater than unity. Suppose that $e_1 > 1$, so that $\mathfrak{o}p$ is divisible by at least the square of $\mathfrak{p}_1$. Write $\frac{\mathfrak{o}p}{\mathfrak{p}_1^2} = \mathfrak{g}$, where $\mathfrak{g}$ is an integral ideal and $\mathfrak{o}p = \mathfrak{p}_1^2\mathfrak{g}$.

Let ω be an integer that is divisible by $\mathfrak{p}_1\mathfrak{g}$ but *not* by $\mathfrak{p}_1^2\mathfrak{g}$. (Vol. I, Art. 215.) Observe that ω is *not* divisible by $\mathfrak{o}p$ or by p, although ω^2 is divisible by p.

Let η be an arbitrary algebraic integer that is divisible by ω. It follows that η^p is divisible by p, and also $\frac{\eta^p}{p}$ is an algebraic integer. If the conjugate quantities of η be $\eta', \eta'', \cdots, \eta^{(n)}$ (including η), then the quantities $\frac{\eta'^p}{p}, \frac{\eta''^p}{p}, \cdots, \frac{\eta^{(n)p}}{p}$ are algebraic integers. For these quantities satisfy the same algebraic equation as is satisfied by $\frac{\eta^p}{p}$. Hence also

$$\frac{\eta'^p}{p} + \frac{\eta''^p}{p} + \cdots + \frac{\eta^{(n)p}}{p} = S\left(\frac{\eta^p}{p}\right)$$

is an algebraic integer. On the other hand, the spur of an algebraic integer is a rational integer, so that

$$S\left(\frac{\eta^p}{p}\right) = S\frac{(\eta^p)}{p}$$

is a rational integer. It follows that $S(\eta^p)$ is divisible by p. Since

$$S(\eta) = \eta' + \eta'' + \cdots + \eta^{(n)},$$

it follows from the lemma of the preceding article, that

$$[S(\eta)]^p \equiv \eta'^p + \eta''^p + \cdots + \eta^{(n)^p} \pmod{p}$$
$$\equiv S(\eta^p) \pmod{p}.$$

From Fermat's Theorem it follows that

$$S(\eta)^p \equiv S(\eta) \pmod{p}.$$

We have therefore

$$S(\eta^p) \equiv S(\eta) \pmod{p}.$$

And, since $S(\eta^p)$ is divisible by p, it follows that $S(\eta)$ is divisible by p. In other words, if η is an algebraic integer that is divisible by ω, then is $S(\eta)$ divisible by p. Note that ω was an algebraic integer that was not divisible by p, although ω^2 was divisible by p.

Since

$$\mathfrak{o} = [\omega_1, \omega_2, \cdots, \omega_n],$$

and since ω is an integer in Ω, it is seen that

$$\omega = x_1\omega_1 + x_2\omega_2 + \cdots + x_n\omega_n, \tag{1}$$

where the x's are all rational integers. These integers $x_1, x_2, \cdots, x_n$ cannot all be divisible by p, otherwise ω would be divisible by p, which is contrary to the hypothesis. Suppose then that x_1 is *not* divisible by p. Since every algebraic integer η which is divisible by ω is such that $S(\eta)$ is divisible by p, it is evident that $S(\omega\omega_r)(r=1, 2, \cdots, n)$ are numbers that are divisible by p.

Giving to ω the value indicated in formula (1), it is seen that

$$S(\omega\omega_r) = x_1 S(\omega_r\omega_1) + x_2 S(\omega_r\omega_2) + \cdots + x_n S(\omega_r\omega_n) \quad (r=1, 2, \cdots, n).$$

On the other hand

$$D = \begin{vmatrix} S(\omega_1\omega_1), & S(\omega_1\omega_2), & \cdots, & S(\omega_1\omega_n) \\ S(\omega_2\omega_1), & S(\omega_2\omega_2), & \cdots, & S(\omega_2\omega_n) \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ S(\omega_n\omega_1), & S(\omega_n\omega_2), & \cdots, & S(\omega_n\omega_n) \end{vmatrix}.$$

Multiply the determinant by x_1, and to the first column add the second column multiplied by x_2, the third multiplied by x_3, $\cdots$, and the nth column multiplied by x_n. It follows that

$$x_1 D = \begin{vmatrix} \sum_{\nu=1}^{\nu=n} [x_\nu S(\omega_1\omega_\nu)], & S(\omega_1\omega_2), & \cdots, & S(\omega_1\omega_n) \\ \sum_{\nu=1}^{\nu=n} [x_\nu S(\omega_2\omega_\nu)], & S(\omega_2\omega_2), & \cdots, & S(\omega_2\omega_n) \\ \cdots\cdots\cdots\

ART. **32.** THEOREM. *If* $\mathfrak{i}$ *is an arbitrary integral ideal, and if* α *and* β *are two algebraic integers of* Ω, *which are congruent* (*mod.* $\mathfrak{i}$), *then is*

$$\mathfrak{o}\alpha+\mathfrak{i}=\mathfrak{o}\beta+\mathfrak{i}.$$

For, since

$$\alpha\equiv\beta \pmod{\mathfrak{i}},$$

it follows that

$$\alpha=\beta+\iota,$$

where ι is an integer divisible by $\mathfrak{i}$. Let $\mathfrak{d}$ be any divisor of $\mathfrak{o}\alpha$ and of $\mathfrak{i}$. It follows that $\mathfrak{i}>\mathfrak{d}$, and consequently ι is divisible by $\mathfrak{d}$. On the other hand, $\mathfrak{o}\alpha$ is divisible by $\mathfrak{d}$, so that α is also divisible by $\mathfrak{d}$. Hence $\alpha-\iota$, or β, is divisible by $\mathfrak{d}$. Thus it is shown that $\mathfrak{o}\beta$ is divisible by $\mathfrak{d}$. It follows that every common divisor of $\mathfrak{o}\alpha$ and of $\mathfrak{i}$, is also a divisor of $\mathfrak{o}\beta$ and of $\mathfrak{i}$. In the same way it is seen that every divisor of $\mathfrak{o}\beta$ and of $\mathfrak{i}$ is also a divisor of $\mathfrak{o}\alpha$ and of $\mathfrak{i}$. And from this it is evident that the greatest common divisor of $\mathfrak{o}\alpha$ and of $\mathfrak{i}$ is the greatest common divisor of $\mathfrak{o}\beta$ and of $\mathfrak{i}$. It follows that

$$\mathfrak{o}\alpha+\mathfrak{i}=\mathfrak{o}\beta+\mathfrak{i},$$

if

$$\alpha\equiv\beta \pmod{\mathfrak{i}}.$$

ART. **33. A Complete Set of Incongruent Residues.** We are now in a position to distribute the numbers that are divisible by $\mathfrak{o}$, and that is, the algebraic integers of Ω into classes with respect to $\mathfrak{i}$ as a modulus. The number of these classes was denoted (Vol. I, Art. 137) by $(\mathfrak{o}, \mathfrak{i})$.

Take an arbitrary integer α which is divisible by $\mathfrak{o}$, and write down all numbers of the form $\alpha+\iota$, where ι is a number divisible by $\mathfrak{i}$. These numbers form a class. If there are in Ω still other integers which do not appear in the complex $\alpha+\iota$, let such an integer be β. Form the complex $\beta+\iota$, etc. Two such complexes are, in virtue of the theorem of the preceding article, either completely

identical, that is, they contain the same numbers; or, they have no number in common. In this distribution of the integers in Ω, we thus have $(\mathfrak{o}, \mathfrak{i})$ different classes or complexes. If, further, we take from each of the $(\mathfrak{o}, \mathfrak{i})$ classes an arbitrary number as a representative of that class, we have a so-called *complete system* (Vol. I, Art. 138) *of incongruent residues* (mod. $\mathfrak{i}$).

Next let α be an integer in Ω, such that

$$\mathfrak{o}\alpha + \mathfrak{i} = \mathfrak{o},$$

and that is, $\mathfrak{o}\alpha$ and $\mathfrak{i}$ are relatively prime; or, as we may say more briefly, α is *relatively* prime to the ideal $\mathfrak{i}$. It follows that all integers of the complex $\mathfrak{o}\alpha + \mathfrak{i}$ are relatively prime to $\mathfrak{i}$, if α is relatively prime to $\mathfrak{i}$. The number of these complexes, which contain only such numbers as are relatively prime to the integral ideal $\mathfrak{i}$, is denoted by $\varphi(\mathfrak{i})$; and that is, $\varphi(\mathfrak{i})$ denotes the number of those integers in Ω, which are incongruent (mod. $\mathfrak{i}$) and which are relatively prime to $\mathfrak{i}$. This function $\varphi(\mathfrak{i})$ has the same significance as the corresponding function in the elementary Theory of Numbers.

THEOREM. *If* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are two integral ideals that are relatively prime, then is*

$$\varphi(\mathfrak{a}\mathfrak{b}) = \varphi(\mathfrak{a})\varphi(\mathfrak{b}).$$

That there may exist an algebraic integer ω which satisfies simultaneously the two congruences

$$\omega \equiv \rho \pmod{\mathfrak{a}},$$
$$\omega \equiv \sigma \pmod{\mathfrak{b}},$$

where ρ and σ are integers of Ω, it is necessary and sufficient (Vol. I, Art. 143), if $\mathfrak{d} = \mathfrak{a} + \mathfrak{b}$, that

$$\rho \equiv \sigma \pmod{\mathfrak{d}}.$$

It was also proved that, if this condition was satisfied, there was an algebraic integer ω_0 in Ω, which simul-

taneously satisfied the two congruences

$$\omega_0 \equiv \rho \pmod{\mathfrak{a}},$$
$$\omega_0 \equiv \sigma \pmod{\mathfrak{b}}.$$

The general solution of these two congruences was shown to be (Vol. I, Art. 143)

$$\omega \equiv \omega_0 \pmod{\mathfrak{m}},$$

where

$$\mathfrak{m} = \mathfrak{a} - \mathfrak{b}.$$

The above result may be applied at once to the special case where $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime. For this case it is seen that (Art. 10)

$$\mathfrak{a} + \mathfrak{b} = \mathfrak{o} \qquad \text{and} \qquad \mathfrak{a} - \mathfrak{b} = \mathfrak{a}\mathfrak{b}.$$

If α and β are two integers of Ω, and if the two following congruences are considered, namely,

$$\omega \equiv \alpha \pmod{\mathfrak{a}},$$
$$\omega \equiv \beta \pmod{\mathfrak{b}},$$

it is evident that they may be satisfied simultaneously. For the necessary condition

$$\alpha \equiv \beta \pmod{\mathfrak{o}}$$

is here of itself satisfied, since $\alpha - \beta$ is an algebraic integer and therefore, divisible by $\mathfrak{o}$. If further ω_0 is a solution of these two congruences, the general solution is

$$\omega \equiv \omega_0 \pmod{\mathfrak{a}\mathfrak{b}}.$$

Write down a system of integers of the realm Ω, which are incongruent (mod. $\mathfrak{a}$) and which are relatively prime to $\mathfrak{a}$. Suppose that this system contains the $\varphi(\mathfrak{a})$ integers $\alpha_1, \alpha_2, \cdots, \alpha_{\varphi(\mathfrak{a})}$. Similarly, write down the system of integers which are incongruent (mod. $\mathfrak{b}$) and which are relatively prime to $\mathfrak{b}$. Denote this system of integers by $\beta_1, \beta_2, \cdots, \beta_{\varphi(\mathfrak{b})}$. From each of these two systems select integers, say, α_r and β_s, and so determine

an algebraic integer of the realm that the two congruences

$$\omega \equiv \alpha_r \pmod{\mathfrak{a}},$$
$$\omega \equiv \beta_s \pmod{\mathfrak{b}},$$

are satisfied. Then let r take one after the other the values $1, 2, \cdots, \varphi(\mathfrak{a})$; and independently of these values, let s take the values $1, 2, \cdots, \varphi(\mathfrak{b})$. Each time an algebraic integer ω is to be determined which satisfies the corresponding congruences. We thus have the $\varphi(\mathfrak{a})\varphi(\mathfrak{b})$ integers

$$\omega_1, \omega_2, \cdots, \omega_{\varphi(\mathfrak{a})\varphi(\mathfrak{b})}.$$

These integers are incongruent (mod. $\mathfrak{ab}$). For, suppose that ω_μ satisfies the two congruences

$$\omega \equiv \alpha_r \pmod{\mathfrak{a}},$$
$$\omega \equiv \beta_s \pmod{\mathfrak{b}};$$

then, if ω_μ were congruent (mod. $\mathfrak{ab}$) to ω_ν, which satisfies the two congruences

$$\omega \equiv \alpha_{r'} \pmod{\mathfrak{a}},$$
$$\omega \equiv \beta_{s'} \pmod{\mathfrak{b}},$$

it would follow, since $\omega_\mu \equiv \omega_\nu \pmod{\mathfrak{a}}$, that

$$\alpha_r \equiv \alpha_{r'} \pmod{\mathfrak{a}},$$

and also

$$\beta_s \equiv \beta_{s'} \pmod{\mathfrak{b}}.$$

But since $\alpha_1, \alpha_2, \cdots, \alpha_{\varphi(\mathfrak{a})}$ are incongruent (mod. $\mathfrak{a}$), and the numbers $\beta_1, \beta_2, \cdots, \beta_{\varphi(\mathfrak{b})}$ are incongruent (mod. $\mathfrak{b}$), it follows that r must be equal to r', and that s must be equal to s'.

It may next be shown that the numbers $\omega_1, \omega_2, \cdots, \omega_{\varphi(\mathfrak{a})\varphi(\mathfrak{b})}$ are relatively prime to $\mathfrak{ab}$. For, since $\alpha_1, \alpha_2, \cdots, \alpha_{\varphi(\mathfrak{a})}$ are all relatively prime to $\mathfrak{a}$; and since every one of the ω's is congruent (mod. $\mathfrak{a}$) to one of these α's, it follows that all the ω's are relatively prime to $\mathfrak{a}$. In a similar manner it is seen that all the ω's are relatively

prime to $\mathfrak{b}$. Hence it follows that all the ω's are relatively prime to the product $\mathfrak{ab}$.

Finally, it may be proved that every integer in Ω, which is relatively prime to $\mathfrak{ab}$, is congruent to one of the numbers $\omega_1, \omega_2, \cdots, \omega_{\varphi(\mathfrak{a})\varphi(\mathfrak{b})}$. For, if ξ is an algebraic integer in Ω that is relatively prime to $\mathfrak{ab}$, it is also relatively prime to both $\mathfrak{a}$ and $\mathfrak{b}$. Hence ξ is congruent to one of the numbers $\alpha_1, \alpha_2, \cdots, \alpha_{\varphi(\mathfrak{a})}$ (mod. $\mathfrak{a}$) and to one of the numbers $\beta_1, \beta_2, \cdots, \beta_{\varphi(\mathfrak{b})}$ (mod. $\mathfrak{b}$), and consequently ξ must satisfy two congruences of the form

$$\xi \equiv \alpha_r \text{ (mod. } \mathfrak{a}),$$

$$\xi \equiv \beta_r \text{ (mod. } \mathfrak{b}).$$

On the other hand all solutions of two such congruences must be congruent (mod. $\mathfrak{ab}$) to one of the numbers $\omega_1, \omega_2, \cdots, \omega_{\varphi(\mathfrak{a})\varphi(\mathfrak{b})}$. From this it is seen that the quantities $\omega_1, \omega_2, \cdots, \omega_{\varphi(\mathfrak{a})\varphi(\mathfrak{b})}$ form a complete system of quantities which are incongruent (mod. $\mathfrak{ab}$), and which are relatively prime to $\mathfrak{ab}$. Such a system is composed of $\varphi(\mathfrak{ab})$ quantities. On the other hand, it was seen that this number is equal to $\varphi(\mathfrak{a})\varphi(\mathfrak{b})$. It follows then that

$$\varphi(\mathfrak{a} \cdot \mathfrak{b}) = \varphi(\mathfrak{a})\varphi(\mathfrak{b}).$$

Observe that $\varphi(\mathfrak{o})$ must by definition be equal to unity.

ART. **34.** The theorem of the preceding article may be extended at once to the product of several ideals. For, if $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \cdots$ are integral ideals which are relatively prime to one another, then

$$\varphi(\mathfrak{abcd} \cdots) = \varphi(\mathfrak{a})\varphi(\mathfrak{bcd} \cdots).$$

This follows at once, for $\mathfrak{a}$ being relatively prime to each of the ideals $\mathfrak{b}, \mathfrak{c}, \mathfrak{d}, \cdots$, is relatively prime to their product. Similarly it is seen that

$$\varphi(\mathfrak{bcd} \cdots) = \varphi(\mathfrak{b})\varphi(\mathfrak{cd} \cdots), \text{ etc.}$$

It is evident from this formula that the calculation of $\varphi(\mathfrak{i})$ is reduced to the case where $\mathfrak{i}$ is the power of a prime ideal. For, if we suppose that $\mathfrak{i}$ is decomposed into prime ideals, say

$$\mathfrak{i} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r},$$

it follows from the above formula, that

$$\varphi(\mathfrak{i}) = \varphi(\mathfrak{p}_1^{e_1})\varphi(\mathfrak{p}_2^{e_2})\cdots\varphi(\mathfrak{p}_r^{e_r}).$$

It is necessary therefore to calculate $\varphi(\mathfrak{i})$ only for the case where $\mathfrak{i}$ is the power of a prime ideal, say

$$\mathfrak{i} = \mathfrak{p}^e.$$

Suppose that the numbers which are divisible by $\mathfrak{o}$, that is, the algebraic integers in Ω are distributed into classes (mod. $\mathfrak{i}$). The number of these classes is $(\mathfrak{o}, \mathfrak{p}^e)$. From each of these $(\mathfrak{o}, \mathfrak{p}^e)$ classes select a quantity as representative of its class. How many of these $(\mathfrak{o}, \mathfrak{p}^e)$ representatives have a common divisor with $\mathfrak{i} = \mathfrak{p}^e$? If a number α which is divisible by $\mathfrak{o}$ has a divisor in common with $\mathfrak{p}^e$, it is evident that α must be divisible by $\mathfrak{p}$. Reciprocally, if α is divisible by $\mathfrak{p}$, then $\mathfrak{i}(=\mathfrak{p}^e)$ and α have a common divisor. The question raised is therefore identical with the following: How many algebraic integers are there in Ω which are divisible by $\mathfrak{p}$ and are incongruent (mod. $\mathfrak{i}$)? Or, how many incongruent integers (mod. $\mathfrak{i}$) are there in Ω which are divisible by $\mathfrak{p}$? We know that there are $(\mathfrak{p}, \mathfrak{i})$ such integers. Hence, if we omit these $(\mathfrak{p}, \mathfrak{i})$ numbers from the above system of representatives, there remain the $\varphi(\mathfrak{i})$ numbers required.

It is thus seen that

$$\varphi(\mathfrak{i}) = (\mathfrak{o}, \mathfrak{i}) - (\mathfrak{p}, \mathfrak{i}) \qquad \text{or} \qquad \varphi(\mathfrak{p}^e) = (\mathfrak{o}, \mathfrak{p}^e) - (\mathfrak{p}, \mathfrak{p}^e).$$

It was proved (Vol. I, Art. 140) that if $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ are three moduls such that

$$\mathfrak{b} > \mathfrak{a}, \qquad \mathfrak{c} > \mathfrak{b},$$

then

$$(\mathfrak{a}, \mathfrak{b})(\mathfrak{b}, \mathfrak{c}) = (\mathfrak{a}, \mathfrak{c}).$$

Since here

$$\mathfrak{i} > \mathfrak{p} \qquad \text{and} \qquad \mathfrak{p} > \mathfrak{o},$$

we have

$$(\mathfrak{o}, \mathfrak{p})(\mathfrak{p}, \mathfrak{i}) = (\mathfrak{o}, \mathfrak{i}) \qquad \text{or} \qquad (\mathfrak{p}, \mathfrak{i}) = \frac{(\mathfrak{o}, \mathfrak{i})}{(\mathfrak{o}, \mathfrak{p})}.$$

It follows that

$$\varphi(\mathfrak{i}) = (\mathfrak{o}, \mathfrak{i})\left\{1 - \frac{1}{(\mathfrak{o}, \mathfrak{p})}\right\} = N(\mathfrak{i})\left\{1 - \frac{1}{N(\mathfrak{p})}\right\};$$

or

$$\varphi(\mathfrak{p}^e) = N(\mathfrak{p}^e) - \frac{N(\mathfrak{p}^e)}{N(\mathfrak{p})} = N(\mathfrak{p})^e - N(\mathfrak{p})^{e-1}.$$

If further $\mathfrak{i}$ is an arbitrary ideal of the realm Ω, and, when decomposed into prime ideals, becomes

$$\mathfrak{i} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_r^{e_r},$$

then from above

$$\varphi(\mathfrak{i}) = \varphi(\mathfrak{p}_1^{e_1})\varphi(\mathfrak{p}_2^{e_2}) \cdots \varphi(\mathfrak{p}_r^{e_r}) = \prod_{\nu=1}^{\nu=r} \varphi(\mathfrak{p}_\nu^{e_\nu})$$

$$= \prod_{\nu=1}^{\nu=r} N(\mathfrak{p}_\nu)^{e_\nu}\left\{1 - \frac{1}{N(\mathfrak{p}_\nu)}\right\} = N(\mathfrak{i}) \prod_{\nu=1}^{\nu=r}\left\{1 - \frac{1}{N(\mathfrak{p}_\nu)}\right\}.$$

If further p_ν is the smallest rational integer that is divisible by $\mathfrak{p}_\nu$, then (Art. 29) is

$$N(\mathfrak{p}_\nu) = p_\nu^{f_\nu};$$

and consequently

$$\varphi(\mathfrak{i}) = \Pi\left(p_\nu^{e_\nu f_\nu}\left\{1 - \frac{1}{p_\nu^{f_\nu}}\right\}\right).$$

ART. **35.** The theorem expressed through the formula

$$\sum \varphi(\mathfrak{d}) = N(\mathfrak{i}),$$

where $\mathfrak{d}$ denotes a divisor of $\mathfrak{i}$, may be proved here.

Write $\mathfrak{i}$ in the form

$$\mathfrak{i} = \mathfrak{i}_1\mathfrak{i}_2,$$

where $\mathfrak{i}_1$ and $\mathfrak{i}_2$ are integral ideals that are relatively prime, and consider a prime factor $\mathfrak{p}^e$ of $\mathfrak{i}$. This factor is a divisor of either $\mathfrak{i}_1$ or of $\mathfrak{i}_2$, but not of both, since $\mathfrak{i}_1$ and $\mathfrak{i}_2$

are relatively prime. We may therefore write

$$\mathfrak{d} = \mathfrak{d}_1 \mathfrak{d}_2,$$

and, as $\mathfrak{d}$ goes through the divisors of $\mathfrak{i}$, let $\mathfrak{d}_1$ go through all divisors of $\mathfrak{i}_1$, while $\mathfrak{d}_2$ goes through all divisors of $\mathfrak{i}_2$. Observe that $\mathfrak{d}_1$ and $\mathfrak{d}_2$ are relatively prime, so that

$$\varphi(\mathfrak{d}_1 \mathfrak{d}_2) = \varphi(\mathfrak{d}_1)\varphi(\mathfrak{d}_2).$$

Since $\mathfrak{d}_1$ and $\mathfrak{d}_2$ are independent of each other, it follows that

$$\sum\{\varphi(\mathfrak{d}_1)\varphi(\mathfrak{d}_2)\} = \sum\varphi(\mathfrak{d}_1) \cdot \sum\varphi(\mathfrak{d}_2);$$

and consequently

$$\sum\varphi(\mathfrak{d}) = \sum\varphi(\mathfrak{d}_1) \cdot \sum\varphi(\mathfrak{d}_2),$$

where $\mathfrak{d}$ takes in all divisors of $\mathfrak{i}$, while $\mathfrak{d}_1$ and $\mathfrak{d}_2$ go through all divisors of $\mathfrak{i}_1$ and of $\mathfrak{i}_2$, respectively.

If then it is assumed that the formula stated at the beginning of this article is proved for $\mathfrak{i}_1$ and for $\mathfrak{i}_2$, that is, if

$$\sum\varphi(\mathfrak{d}_1) = N(\mathfrak{i}_1) \qquad \text{and} \qquad \sum\varphi(\mathfrak{d}_2) = N(\mathfrak{i}_2),$$

it follows that (Art. 22)

$$\sum\varphi(\mathfrak{d}) = N(\mathfrak{i}_1)N(\mathfrak{i}_2) = N(\mathfrak{i}).$$

Hence, to prove the formula

$$\sum\varphi(\mathfrak{d}) = N(\mathfrak{i}),$$

in its generality, it is necessary only to show that it is true for the case in which $\mathfrak{i}$ is the power of a prime ideal.

Suppose then that

$$\mathfrak{i} = \mathfrak{p}^e,$$

where $\mathfrak{p}$ is a prime ideal, e being a positive rational integer. The divisors which $\mathfrak{d}$ can go through are

$$\mathfrak{o}, \mathfrak{p}, \mathfrak{p}^2, \cdots, \mathfrak{p}^e;$$

and it is clear that

$$\begin{aligned}\sum\varphi(\mathfrak{d}) &= \varphi(\mathfrak{o}) + \varphi(\mathfrak{p}) + \varphi(\mathfrak{p}^2) + \cdots + \varphi(\mathfrak{p}^e) \\ &= 1 + N(\mathfrak{p}) - 1 + N(\mathfrak{p}^2) - N(\mathfrak{p}) + N(\mathfrak{p}^3) - N(\mathfrak{p}^2) \\ &\quad + \cdots + N(\mathfrak{p}^e) - N(\mathfrak{p}^{e-1}).\end{aligned}$$

Hence it is evident that

$$\sum \varphi(\mathfrak{d}) = N(\mathfrak{p}^e) = N(\mathfrak{i}).$$

As it has been shown that this formula, when true individually of two ideals $\mathfrak{i}_1$ and $\mathfrak{i}_2$, which are relatively prime, is true also of their product, it is seen that the formula is true in general.

ART. **36. Fermat's Theorem.** *Let* $\mathfrak{i}$ *be any integral ideal and let* ω *be an integer that is relatively prime to* $\mathfrak{i}$, *then is*

$$\omega^{\varphi(\mathfrak{i})} \equiv 1 \pmod{\mathfrak{i}}.$$

Put

$$r = \varphi(\mathfrak{i}).$$

Further, let the algebraic integers $\omega_1, \omega_2, \cdots, \omega_r$ form a system of incongruent integers (mod. $\mathfrak{i}$), which are relatively prime to $\mathfrak{i}$. Let one of these r integers be ω, and form the products $\omega\omega_1, \omega\omega_2, \cdots, \omega\omega_r$. The integers are also relatively prime to $\mathfrak{i}$. Further, they are incongruent (mod. $\mathfrak{i}$) to one another. For, if

$$\omega\omega_\rho \equiv \omega\omega_\sigma \pmod{\mathfrak{i}},$$

where ρ, σ are any two of the numbers $1, 2, \cdots, r$ that are different from one another, then is

$$\omega_\rho \equiv \omega_\sigma \pmod{\mathfrak{i}}.$$

This, however, contradicts the assumption regarding ω_ρ and ω_σ. It is thus seen that the numbers $\omega\omega_1, \omega\omega_2, \cdots, \omega\omega_r$ form a complete system of incongruent (mod. $\mathfrak{i}$) residues; and consequently, neglecting the sequence, are congruent (mod. $\mathfrak{i}$) to the numbers $\omega_1, \omega_2, \cdots, \omega_r$. We thus have

$$\begin{aligned} \omega\omega_1 &\equiv \omega_\rho \pmod{\mathfrak{i}}, \\ \omega\omega_2 &\equiv \omega_\sigma \pmod{\mathfrak{i}}, \\ &\cdots\cdots\cdots\cdots \\ \omega\omega_r &\equiv \omega_\tau \pmod{\mathfrak{i}}, \end{aligned}$$

$\rho, \sigma, \cdots, \tau$ being the numbers $1, 2, \cdots, r$, when the latter

are arranged in a certain sequence. If both sides of these congruences are multiplied together, we have

$$\omega^r\omega_1\omega_2\cdots\omega_r \equiv \omega_1\omega_2\cdots\omega_r \pmod{\mathfrak{i}};$$

and since $\omega_1\omega_2\cdots\omega_r$ is relatively prime to $\mathfrak{i}$, it follows that

$$\omega^r \equiv 1 \pmod{\mathfrak{i}},$$

and that is the Fermat Theorem

$$\omega^{\varphi(\mathfrak{i})} \equiv 1 \pmod{\mathfrak{i}}.$$

This theorem is true *only* for an integer ω which is relatively prime to $\mathfrak{i}$.

If next the special case is considered, where $\mathfrak{i}$ is a prime ideal, say, $\mathfrak{p}$ of degree f; and if p is the least rational number divisible by $\mathfrak{p}$, then is

$$N(\mathfrak{i}) = N(\mathfrak{p}) = p^f;$$

and consequently

$$\varphi(\mathfrak{i}) = p^f - 1.$$

It follows at once from Fermat's Theorem that

$$\omega^{p^f-1} \equiv 1 \pmod{\mathfrak{p}}.$$

For this special case the theorem may be put in such a form that it is true for every algebraic integer ω in Ω. For, multiply the congruence by ω. We then have

$$\omega^{p^f} \equiv \omega \pmod{\mathfrak{p}} \qquad \text{or} \qquad \omega^{N(\mathfrak{p})} \equiv \omega \pmod{\mathfrak{p}};$$

and in this form the theorem is also true for the case that ω is divisible by the prime ideal $\mathfrak{p}$ and consequently true in general for every integer ω in Ω. It is evident, for example, that every integer ω that is not divisible by the prime ideal $\mathfrak{p}$ of degree f satisfies the congruence

$$\omega^{p^f(p^f-1)} \equiv 1 \pmod{\mathfrak{p}^2}.$$

ART. 37. **Congruences of the *m*th Degree in a Realm of the *m*th Degree.**

Let

$$f(x) = \alpha_0 x^m + \alpha_1 x^{m-1} + \cdots + \alpha_m,$$

where $\alpha_0, \alpha_1, \cdots, \alpha_m$ are algebraic integers of Ω, and x

is a variable. If there is an algebraic integer in Ω, such that

$$f(\omega) \equiv 0 \pmod{\mathfrak{p}},$$

then ω is a *root* of the congruence

$$f(x) \equiv 0 \pmod{\mathfrak{p}}.$$

If ω is a root of the congruence

$$f(x) \equiv 0 \pmod{\mathfrak{p}},$$

then also is ω' a root of the same congruence, if

$$\omega' \equiv \omega \pmod{\mathfrak{p}}.$$

Two roots of this congruence are regarded as different only when they are incongruent (mod. $\mathfrak{p}$). The coefficients of the congruence, $\alpha_0, \alpha_1, \cdots, \alpha_m$ are determined (mod. $\mathfrak{p}$) only. That is, they may be replaced by other algebraic integers of Ω, which are congruent to them (mod. $\mathfrak{p}$). If then the coefficient of a term is divisible by $\mathfrak{p}$, this term may be omitted in the congruence. Hence, in the congruence

$$\alpha_0 x^m + \alpha_1 x^{m-1} + \cdots + \alpha_m \equiv 0 \pmod{\mathfrak{p}}$$

the exponent of the highest term (the degree of the congruence) is m only when α_0 is *not* divisible by $\mathfrak{p}$. Thus the *degree* of the congruence is determined by the exponent of the first term whose coefficient is not divisible by $\mathfrak{p}$.

THEOREM. *If the modulus of a congruence of the mth degree is a prime ideal* $\mathfrak{p}$, *this congruence has at most m incongruent (mod.* $\mathfrak{p}$*) roots.*

This theorem is proved first for the special case where $m = 1$. The congruence is then

$$\alpha_0 x + \alpha_1 \equiv 0 \pmod{\mathfrak{p}},$$

where α_0 is *not* divisible by $\mathfrak{p}$. Let ω and ω' be two of its roots, so that

$$\alpha_0 \omega + \alpha_1 \equiv 0 \pmod{\mathfrak{p}},$$
$$\alpha_0 \omega' + \alpha_1 \equiv 0 \pmod{\mathfrak{p}}.$$

It follows that

$$\alpha_0\omega \equiv \alpha_0\omega' \pmod{\mathfrak{p}}.$$

Further, since α_0 is not divisible by $\mathfrak{p}$, and consequently is relatively prime to $\mathfrak{p}$, it is seen that

$$\omega \equiv \omega' \pmod{\mathfrak{p}}.$$

It follows that *a congruence of the first degree can have at most one incongruent root (mod. $\mathfrak{p}$).*

Assume that the theorem to be proved is true for the cases where the degree is less than or equal to $m-1$. On this assumption the theorem may be proved for congruences, whose degree is m. Suppose that

$$f(x) = \alpha_0 x^m + \alpha_1 x^{m-1} + \cdots + \alpha_m,$$

where α_0 is not divisible by $\mathfrak{p}$. If ω is a root of

$$f(x) \equiv 0 \pmod{\mathfrak{p}},$$

it follows that

$$f(x) - f(\omega) = (x-\omega)[\beta_0 x^{m-1} + \beta_1 x^{m-2} + \cdots + \beta_{m-1}] \equiv 0 \pmod{\mathfrak{p}}.$$

If ω and η are two incongruent roots (mod. $\mathfrak{p}$) of $f(x) \equiv 0$ (mod. $\mathfrak{p}$), so that

$$f(\omega) \equiv 0 \pmod{\mathfrak{p}} \qquad \text{and} \qquad f(\eta) \equiv 0 \pmod{\mathfrak{p}},$$

then, from the formula above, we have

$$(\eta-\omega)[\beta_0\eta^{m-1} + \beta_1\eta^{m-2} + \cdots + \beta_{m-1}] \equiv 0 \pmod{\mathfrak{p}}.$$

As η and ω are incongruent (mod. $\mathfrak{p}$), it follows that

$$\beta_0\eta^{m-1} + \beta_1\eta^{m-2} + \cdots + \beta_{m-1} \equiv 0 \pmod{\mathfrak{p}}.$$

This is a congruence of the $(m-1)$st degree in η. Since $\beta_0 = \alpha_0$ is *not* divisible by $\mathfrak{p}$, in view of the above assumption, this congruence can have at most $m-1$ roots. It follows that the original congruence of the mth degree can have at most m roots, which are incongruent (mod. $\mathfrak{p}$). As this theorem was proved for $m=1$, it is seen to be true in general.

Suppose that the congruence

$$f(x)=\alpha_0x^m+\alpha_1x^{m-1}+\cdots+\alpha_m\equiv 0 \pmod{\mathfrak{p}}$$

has exactly m incongruent (mod. $\mathfrak{p}$) roots, say $\xi_1, \xi_2, \cdots, \xi_m$. Consider the congruence

$$\alpha_0x^m+\alpha_1x^{m-1}+\cdots+\alpha_m-\alpha_0(x-\xi_1)(x-\xi_2)\cdots(x-\xi_m)\equiv 0 \pmod{\mathfrak{p}}.$$

This congruence is at most of the $(m-1)$st degree, as the terms in x^m cancel. It has, however, more than $m-1$ incongruent (mod. $\mathfrak{p}$) roots $\xi_1, \xi_2, \cdots, \xi_m$. It follows that all the coefficients of the congruence are divisible by $\mathfrak{p}$, and consequently

$$-\frac{\alpha_1}{\alpha_0}\equiv\xi_1+\xi_2+\cdots+\xi_m \pmod{\mathfrak{p}},$$

$$\frac{\alpha_2}{\alpha_0}\equiv\xi_1\xi_2+\xi_1\xi_3+\cdots+\xi_{m-1}\xi_m \pmod{\mathfrak{p}},$$

$$-\frac{\alpha_3}{\alpha_0}\equiv\xi_1\xi_2\xi_3+\xi_1\xi_2\xi_4+\cdots+\xi_{m-2}\xi_{m-1}\xi_m \pmod{\mathfrak{p}},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$(-1)^m\frac{\alpha_m}{\alpha_0}\equiv\xi_1\xi_2\cdots\xi_m \pmod{\mathfrak{p}}.$$

The following theorem has thus been proved. *If the congruence of the mth degree* $f(x)\equiv 0$ *(mod.* $\mathfrak{p}$*) has exactly* m *roots, say,* $\xi_1, \xi_2, \cdots, \xi_m$, *there exists the identical congruence*

$$f(x)\equiv\alpha_0\prod_{r=1}^{r=m}(x-\xi_r) \pmod{\mathfrak{p}}.$$

ART. **38. Wilson's Theorem.** The above theorem may be applied to the special case

$$f(x)=x^{p^f-1}\equiv 1 \pmod{\mathfrak{p}},$$

where p is the smallest rational integer that is divisible by the prime ideal $\mathfrak{p}$, and where f is its degree (Art. 29). This congruence may be written in the form

$$x^{N(\mathfrak{p})-1}\equiv 1 \pmod{\mathfrak{p}}.$$

There are p^f-1 incongruent roots (mod. $\mathfrak{p}$). For, the congruence is satisfied, due to the Fermat Theorem, by all the incongruent (mod. $\mathfrak{p}$) integers of Ω that are relatively prime to $\mathfrak{p}$, and this number is

$$\varphi(\mathfrak{p}) = N(\mathfrak{p}) - 1.$$

It follows from the theorem of the preceding article that

$$x^{p^f-1} \equiv \Pi(x-\omega) \pmod{\mathfrak{p}},$$

where the product is to be taken over a system of incongruent (mod. $\mathfrak{p}$) numbers ω, that are relatively prime to $\mathfrak{p}$. This, being an identical congruence, is consequently true for all values of x, so that when $x=0$, it follows that

$$1 \equiv \Pi\omega \pmod{\mathfrak{p}},$$

where the product is to be taken as just described. This may be called the *Wilson Theorem*, as it is the analogue of the Wilson Theorem in rational numbers.

ART. 39. **The Height of an Algebraic Integer.** If the following series of numbers is considered, namely,

$$\omega(=\omega^{p^0}),\ \omega^{p^1},\ \omega^{p^2},\ \cdots$$

where ω is an arbitrary integer of the realm Ω, and p is the smallest prime integer divisible by $\mathfrak{p}$, we must finally come to a number r such that

$$\omega^{p^r} \equiv \omega^{p^0} \pmod{\mathfrak{p}}.$$

If this number r is not reached earlier in the series, we have it at all events for $r=f$, where f is the degree of $\mathfrak{p}$.

We shall call the smallest rational integer h, which is different from zero and which satisfies the congruence

$$\omega^{p^h} \equiv \omega \pmod{\mathfrak{p}},$$

the *height* of ω.

If h is the height of ω, it follows at once, by raising the above congruence to the p^h power, that

$$\omega^{p^h p^h} \equiv \omega^{p^h} \pmod{\mathfrak{p}}, \qquad \text{or} \qquad \omega^{p^{2h}} \equiv \omega \pmod{\mathfrak{p}};$$

and similarly

$$\omega^{p^{2h}} \equiv \omega \pmod{\mathfrak{p}},$$
$$\omega^{p^{3h}} \equiv \omega \pmod{\mathfrak{p}},$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$\omega^{p^{mh}} \equiv \omega \pmod{\mathfrak{p}}.$$

If this last congruence is raised to the p^r power, it is seen that

$$\omega^{p^{mh+r}} \equiv \omega^{p^r} \pmod{\mathfrak{p}}.$$

Put

$$mh+r=s, \qquad \text{or} \qquad r \equiv s \pmod{h},$$

and it is evident that

(1) $$\omega^{p^r} \equiv \omega^{p^s} \pmod{\mathfrak{p}}.$$

Reciprocally, it may be proved that if formula (1) is true, then also

$$r \equiv s \pmod{h}.$$

In the proof of this theorem it is necessary to consider only the case where r and s are two of the integers $0, 1, 2, \cdots, h-1$. For, if r and s are two arbitrary integers, we may always find two other integers r' and s' such that

$$r \equiv r' \pmod{h} \qquad \text{and} \qquad s \equiv s' \pmod{h}.$$

Hence, since

$$\omega^{p^r} \equiv \omega^{p^{r'}} \pmod{\mathfrak{p}} \qquad \text{and} \qquad \omega^{p^s} \equiv \omega^{p^{s'}} \pmod{\mathfrak{p}},$$

if

$$\omega^{p^r} \equiv \omega^{p^s} \pmod{\mathfrak{p}},$$

it follows also that

$$\omega^{p^{r'}} \equiv \omega^{p^{s'}} \pmod{\mathfrak{p}},$$

and vice versa. If then r' and s' are two numbers of the series $0, 1, \cdots, h-1$, such that

$$\omega^{p^{r'}} \equiv \omega^{p^{s'}} \pmod{\mathfrak{p}},$$

it may be proved as follows that

$$r' = s'.$$

Suppose that

$$r' \neq s',$$

and let

$$r' = s' + t,$$

where

$$1 \leqq t \leqq h-1.$$

If we raise the congruence

$$\omega^{p^{s'+t}} \equiv \omega^{p^{s'}} \pmod{\mathfrak{p}}$$

to the $p^{h-s'-t}$ power, where $h-s'-t$ is a positive integer, (since $h-r'$ is a positive integer), we have

$$\omega^{p^h} \equiv \omega^{p^{h-t}} \pmod{\mathfrak{p}}.$$

But, since

$$\omega^{p^h} \equiv \omega \pmod{\mathfrak{p}},$$

it follows that

$$\omega^{p^{h-t}} \equiv \omega \pmod{\mathfrak{p}}.$$

Since h is the smallest integer which satisfies the congruence

$$\omega^{p^h} \equiv \omega \pmod{\mathfrak{p}},$$

it follows that $t=0$, and consequently $r' = s'$.

If then r and s are two arbitrary positive integers, which satisfy the congruence

$$\omega^{p^r} \equiv \omega^{p^s} \pmod{\mathfrak{p}},$$

it follows that

$$r \equiv s \pmod{h}.$$

Incidentally, we have proved the following two theorems:

1°. If $s \not\equiv r \pmod{h}$, then $\omega^{p^r} \not\equiv \omega^{p^s} \pmod{\mathfrak{p}}$;
2°. If $\omega^{p^r} \not\equiv \omega^{p^s} \pmod{\mathfrak{p}}$, then $r \not\equiv s \pmod{h}$.

ART. 40. **The Period of an Algebraic Integer.** Consider the infinite series of numbers

$$\omega(=\omega^{p^0}),\ \omega^{p^1},\ \omega^{p^2},\ \omega^{p^3},\ \cdots$$

with respect to the modulus, the prime ideal $\mathfrak{p}$. Observe that the first h of the numbers, where h is the height of ω, are incongruent (mod. $\mathfrak{p}$), while the next h numbers occur

in the same sequence, being the same as the first h numbers. The numbers

$$\omega^{p^0}, \omega^{p^1}, \omega^{p^2}, \cdots, \omega^{p^{h-1}}$$

are said to constitute the *period* of the number ω.

The period of the number ω^{p^r}, where r is any positive rational integer, is $\omega^{p^r}, \omega^{p^{r+1}}, \omega^{p^{r+2}}, \cdots, \omega^{p^{r+h-1}}$. This period of ω^{p^r} contains the same numbers as the period of ω, there being a cyclic change in sequence.

ART. **41.** We may next consider the numbers whose height is unity. These numbers satisfy the congruence

$$\omega^p \equiv \omega \pmod{\mathfrak{p}}.$$

Note that, due to the Fermat Theorem, every rational integer ω satisfies the congruence

$$\omega^p \equiv \omega \pmod{p},$$

where p is any rational prime integer. Consequently, since p is divisible by $\mathfrak{p}$,

$$\omega^p \equiv \omega \pmod{\mathfrak{p}}.$$

We therefore have the theorem: *Every rational integer has the height unity.* Reciprocally, *every number of the height unity is congruent to a rational integer* (*mod.* $\mathfrak{p}$).

Proof. The congruence

$$x^p - x \equiv 0 \pmod{\mathfrak{p}}$$

is satisfied by the p rational integers $0, 1, \cdots, p-1$. These p numbers are incongruent (mod. $\mathfrak{p}$).

For, were

$$r \equiv s \pmod{\mathfrak{p}}$$

where r and s are two of the integers, $0, 1, 2, \cdots, p-1$, it would follow (Art. 29) that $r-s$ is an integral multiple of p. But this cannot be true, since r and s are both less than p. It follows that the congruence

$$x^p - x \equiv 0 \pmod{\mathfrak{p}}$$

has as many incongruent roots (mod. $\mathfrak{p}$) as is the degree of the congruence.

Observe further (Art. 37) that

$$x^p - x \equiv x(x-1)(x-2)\cdots(x-p+1) \pmod{\mathfrak{p}}$$

is an identical congruence. If then ω is a number of the height 1, and as

$$\omega^p - \omega \equiv 0 \pmod{\mathfrak{p}},$$

it follows that

$$\omega(\omega-1)\cdots(\omega-p+1) \equiv 0 \pmod{\mathfrak{p}}.$$

Consequently, we must have

$$\omega \equiv r \pmod{\mathfrak{p}},$$

where r is one of the integers $0, 1, 2, \cdots, p-1$. From this it is seen that ω is congruent to a rational integer r (mod. $\mathfrak{p}$), when the height of ω is 1.

Observe further that, if ω is congruent to a rational integer r (mod. $\mathfrak{p}$), then also

$$\omega^p \equiv r^p \pmod{\mathfrak{p}}.$$

But by the Fermat Theorem

$$r^p \equiv r \pmod{p},$$

consequently also

$$r^p \equiv r \pmod{\mathfrak{p}}.$$

It follows that

$$\omega^p \equiv r \pmod{\mathfrak{p}}.$$

As

$$\omega \equiv r \pmod{\mathfrak{p}},$$

it is clear that

$$\omega^p \equiv \omega \pmod{\mathfrak{p}},$$

and obviously ω has the height unity.

We have thus shown that *every number that is congruent to a rational number* (*mod.* $\mathfrak{p}$) *has the height 1, and that every number which has the height unity is congruent to a rational integer* (*mod.* $\mathfrak{p}$).

ART. **42.** If f is the degree of the prime ideal $\mathfrak{p}$, then (Art. 36)

$$\omega^{p^f} \equiv \omega \pmod{\mathfrak{p}},$$

where ω is any integer in Ω.

If h is the height of ω, then (Art. 39)

$$\omega^{p^h} \equiv \omega \pmod{\mathfrak{p}},$$

and consequently

$$\omega^{p^h} \equiv \omega^{p^f} \pmod{\mathfrak{p}}.$$

But from the theorem in Art. 39 it follows that

$$h \equiv f \pmod{h},$$

and consequently f is divisible by h.

It is thus seen that *the height of every algebraic integer is a divisor of the degree of* $\mathfrak{p}$.

The following question at once arises: If h is an arbitrary divisor of f, do algebraic integers in Ω of the height h always exist? Before answering this question, it is necessary to prove certain lemmas.

Let h be the height of ω, and further let

$$\eta = S(\omega, \omega^p, \omega^{p^2}, \cdots, \omega^{p^{h-1}})$$

be an integral symmetric function of the h quantities $\omega, \omega^p, \omega^{p^2}, \cdots, \omega^{p^{h-1}}$. It is evident that η is an algebraic integer of the realm Ω. It was proved (Art. 30) that if $R(\alpha, \beta, \gamma, \cdots)$ is an arbitrary algebraic function of $\alpha, \beta, \gamma, \cdots$, then

$$[R(\alpha, \beta, \gamma, \cdots)]^p \equiv R(\alpha^p, \beta^p, \gamma^p, \cdots) \pmod{p}.$$

If p is the least rational prime integer that is divisible by the prime ideal $\mathfrak{p}$, then the above congruence is true (mod. $\mathfrak{p}$). It is evident that

$$[S(\omega, \omega^p, \omega^{p^2}, \cdots, \omega^{p^{h-1}}]^p \equiv S(\omega^p, \omega^{p^2}, \omega^{p^3}, \cdots, \omega^{p^h}) \pmod{\mathfrak{p}}.$$

Since S is a symmetric function of its arguments, and since

$$\omega^{p^h} \equiv \omega \pmod{\mathfrak{p}},$$

it is seen that

$$S(\omega^p, \omega^{p^2}, \cdots, \omega^{p^h}) = S(\omega, \omega^p, \omega^{p^2}, \cdots, \omega^{p^{h-1}}) = \eta.$$

It follows that

$$\eta^p \equiv \eta \pmod{\mathfrak{p}},$$

and consequently η has the height unity and is accordingly (Art. 41) congruent to a rational integer (mod. $\mathfrak{p}$).

Thus is proved the lemma: *Every symmetric function of the h quantities*

$$\omega, \omega^p, \omega^{p^2}, \cdots, \omega^{p^{h-1}}$$

is congruent to a rational integer (mod. $\mathfrak{p}$).

Form the product

$$P(x) = (x-\omega)(x-\omega^p)(x-\omega^{p^2})\cdots(x-\omega^{p^{h-1}}),$$

which, when developed in powers of x, gives

$$P(x) = x^h + c_1 x^{h-1} + c_2 x^{h-2} + \cdots + c_{h-1}x + c_h,$$

where the c's, being symmetric functions of $\omega, \omega^p, \omega^{p^2}, \cdots, \omega^{p^{h-1}}$, are congruent to rational integers (mod. $\mathfrak{p}$). It follows that the function $P(x)$ is an integral function of the hth degree whose coefficients are congruent to rational integers (mod. $\mathfrak{p}$). Since every rational integer that is divisible by the prime ideal $\mathfrak{p}$ is also divisible by p, where p is the smallest rational integer that is divisible by the prime ideal $\mathfrak{p}$, it is clear that the coefficients are determined (mod. p) only.

ART. 43. THEOREM. *The function $P(x)$ is a prime function (mod. p), that is, it is impossible to determine two integral functions $f(x)$ and $g(x)$ with rational integral coefficients, such that*

$$P(x) \equiv f(x)g(x) \pmod{p},$$

without one of the functions $f(x)$ or $g(x)$ being constant.

An indirect proof of this theorem will be given. Suppose that there are two functions $f(x)$ and $g(x)$, such that

$$P(x) \equiv f(x)g(x) \pmod{p},$$

where $f(x)$ is of the degree r in x, and $g(x)$ is of degree s, and $r+s$ is equal to h. We then have

$$P(\omega) \equiv f(\omega)g(\omega) \pmod{p};$$

and, since the function $P(x)$ is congruent (mod. p) to the product

$$(x-\omega)(x-\omega^p)(x-\omega^{p^2})\cdots(x-\omega^{p^{h-1}}),$$

it follows that

$$0 \equiv P(\omega) \equiv f(\omega)g(\omega) \pmod{\mathfrak{p}}.$$

Hence, either $f(\omega)$ or $g(\omega)$ is divisible by $\mathfrak{p}$. Assume that $f(\omega)$ is divisible by $\mathfrak{p}$. Then, since

$$f(\omega) \equiv 0 \pmod{\mathfrak{p}},$$

it is seen that

$$f(\omega)^p \equiv 0 \pmod{\mathfrak{p}};$$

and since (Art. 30),

$$f(\omega)^p \equiv f(\omega^p) \pmod{\mathfrak{p}},$$

it follows that

$$f(\omega^p) \equiv 0 \pmod{\mathfrak{p}}.$$

Similarly, it is seen that

$$f(\omega^p)^p \equiv 0 \pmod{\mathfrak{p}};$$

and consequently

$$f(\omega^{2p}) \equiv 0 \pmod{\mathfrak{p}},$$
$$f(\omega^{3p}) \equiv 0 \pmod{\mathfrak{p}},$$
$$\cdots\quad\cdots\quad\cdots\quad\cdots$$
$$\cdots\quad\cdots\quad\cdots\quad\cdots$$

Thus it is seen that the congruence of the rth degree

$$f(x) \equiv 0 \pmod{\mathfrak{p}}$$

is satisfied by all the numbers that constitute the period of ω, namely,

$$\omega,\ \omega^p,\ \omega^{p^2},\ \cdots,\ \omega^{p^{h-1}}.$$

A congruence of the rth degree, however, can have at most r incongruent roots (mod. $\mathfrak{p}$). It follows then that

$$h \leqq r.$$

On the other hand, since

$$h=r+s,$$

it is clear that

$$h=r, \qquad s=0,$$

and consequently $g(x)$ is a constant. At the same time, it is proved that $P(x)$ must be a *prime function* (mod. p).

ART. **44.** We come now to the question of Art. 42. Are there numbers of the height h, where h is any divisor of f; and if so, how many such numbers are there?

If we admit that there is a number ω of the height h, then the numbers of the period of ω,

$$\omega,\ \omega^p,\ \omega^{p^2},\ \cdots,\ \omega^{p^{h-1}}$$

all have the height h. For

$$(\omega^p)^{p^h}\equiv(\omega^{p^h})^p\equiv\omega^p \pmod{\mathfrak{p}}, \text{ etc.},$$

all have the height h. We may consequently distribute all numbers of the height h into groups, there being h numbers in each group. It follows that the number of numbers of the height h must be divisible by h. The number of numbers of the height h may be denoted by $h\chi_h$, where χ_h is a positive integer or zero.

It was seen that the degree of the prime ideal $\mathfrak{p}$ is divisible by h; and that is,

$$f=gh,$$

where g is a positive integer. It follows that p^f-1 is divisible by p^h-1. In fact,

$$\frac{p^f-1}{p^h-1}=1+p^h+p^{2h}+\cdots+p^{(f/h-1)h},$$

which is a positive integer. If further, we put

$$\frac{x^{p^f-1}-1}{x^{p^h-1}-1}=\Phi(x),$$

it is seen that $\Phi(x)$ is an integral function of x with

rational integral coefficients. It also follows that

$$\frac{x^{p^f}-x}{x^{p^h}-x}=\Phi(x); \qquad \text{or} \qquad x^{p^f}-x=\Phi(x)(x^{p^h}-x).$$

The degrees of $x^{p^f}-x$ and of $x^{p^h}-x$ being, respectively p^f and p^h, it is seen that the degree of $\Phi(x)$ is p^f-p^h.

From the theorem of Art. 38 the congruence

$$x^{p^f}-x\equiv 0 \pmod{\mathfrak{p}}$$

has p^f incongruent roots (mod. $\mathfrak{p}$). These roots, because of the identical relation

$$x^{p^f}-x\equiv\Phi(x)(x^{p^h}-x),$$

must satisfy one of the two congruences

$$\Phi(x)\equiv 0 \pmod{\mathfrak{p}} \qquad \text{or} \qquad x^{p^h}-x\equiv 0 \pmod{\mathfrak{p}}.$$

From this it is seen that

$$x^{p^h}-x\equiv 0 \pmod{\mathfrak{p}}$$

cannot have fewer than p^h incongruent roots (mod. $\mathfrak{p}$). For, if there were fewer than this number of roots, the congruence

$$\Phi(x)\equiv 0 \pmod{\mathfrak{p}}$$

must have more than p^f-p^h incongruent roots (mod. $\mathfrak{p}$), which contradicts the theorem of Art. 37. But the congruence

$$x^{p^h}-x\equiv 0 \pmod{\mathfrak{p}}$$

cannot have more than p^h incongruent roots (mod. $\mathfrak{p}$). Therefore, this congruence must have exactly p^h incongruent roots (mod. $\mathfrak{p}$).

ART. **45.** If the number ω satisfies the congruence

$$\omega^{p^h}\equiv\omega \pmod{\mathfrak{p}},$$

it is not necessary that ω have the height h. We can only say that h must be an integral multiple of the height of ω (Art. 39). If then a number ω satisfies the congruence

$$\omega^{p^h}\equiv\omega \pmod{\mathfrak{p}},$$

the height of ω must be either h or a divisor of h. It follows that each of the p^h incongruent numbers (mod. $\mathfrak{p}$), which satisfies the congruence

$$x^{p^h} \equiv \omega \text{ (mod. } \mathfrak{p}),$$

has either the height h or a height which is a divisor of h. If d is a divisor of h, the number of incongruent numbers (mod. $\mathfrak{p}$) of the height d is $d\chi_d$ (Art. 44). Hence, the number of incongruent numbers (mod. $\mathfrak{p}$) whose height is h, or a divisor of h, is had, if in the expression

$$\sum d\chi_d,$$

the summation is taken over all divisors d of h, including h itself. On the other hand, it was seen that this number was p^h. It follows that

$$p^h = \sum d\chi_d.$$

This formula is true also for all divisors of h. For, if h' is a divisor of h, then f is also divisible by h', and there results the analogous formula as above

$$\sum d'\chi_{d'} = p^{h'},$$

where the summation is to be taken over all divisors d' of h'.

Next, introduce the coefficients of Möbius (Vol. I, Art. 201), namely, $\mu(m) = 1$, if $m = 1$; $\mu(m) = 0$, if m is divisible by the square of a number which is different from 1; $\mu(m) = +1$, if m contains as factors an even number of prime factors; $\mu(m) = -1$, if m contains an odd number of different prime factors. We may then write after a well known theorem

$$h\chi_h = \sum \{\mu(d) p^{\frac{h}{d}}\},$$

where the summation is taken over all divisors d of h. Or, more explicitly

$$h\chi_h = p^h - \sum p^{\frac{h}{a}} + \sum p^{\frac{h}{ab}} - \sum p^{\frac{h}{abc}} + \cdots,$$

where the sum $\sum p^{\frac{h}{a}}$ is to be taken over all prime factors a of h, while the sum $\sum p^{\frac{h}{ab}}$ is to be taken over all products of two different prime numbers a and b, which are divisors of h; etc.

It is seen at once that

$$\chi_h > 0;$$

for, the right hand side of the formula just written has the factor $p^{\frac{h}{ab\cdots k}}$, where $a, b, \cdots, k$ are all the prime factors of h. The second factor on the right will contain terms, all of which are divisible by p except the last, which is unity. Hence the second factor is congruent to 1 (mod. p). It follows that χ_h cannot be zero and therefore it must be a positive integer.

It is thus seen that, if h is a divisor of f, there are *always* numbers of the height h.

ART. **46. Primary Prime Functions.**[1] The congruence

$$x^{p^h} - x \equiv 0 \pmod{\mathfrak{p}}$$

has exactly p^h incongruent roots (mod. $\mathfrak{p}$) and is satisfied by all numbers whose height is h, or a divisor of h. It follows from (Art. 38) that

$$x^{p^h} - x \equiv \Pi(x - \omega) \pmod{\mathfrak{p}},$$

where the product is to be taken over a system of p^h incongruent numbers (mod. $\mathfrak{p}$), whose height is h, or a divisor of h. In this product, if ω is a number of the height h, there enters a product

$$(x-\omega)(x-\omega^p)(x-\omega^{p^2})\cdots(x-\omega^{p^{h-1}}),$$

which (Art. 42) may be replaced by a prime function with rational coefficients.

[1] In this connection see the "Report on the Theory of Numbers," by H. J. S. Smith, *Collected Math. Papers.* Vol. I, §§ 69, 70.

Similarly, there enters into the original product a product of the form

$$(x-\omega')(x-\omega'^{p})(x-\omega'^{p^2})\cdots(x-\omega'^{p^{\alpha-1}}),$$

where d is a divisor of h. This last product may also be replaced by a congruent (mod. $\mathfrak{p}$) prime function of degree d, whose coefficients are rational integers.

In short, we may replace the original product through a product of prime functions, and thus have

$$x^{p^h}-x\equiv\Pi P(x)\ (\text{mod. }\mathfrak{p}),$$

where $P(x)$ denotes certain prime functions. Since the coefficients in the product to the right are rational integers, the congruence may also be taken (mod. p), thus giving

$$x^{p^h}-x\equiv\Pi P(x)\ (\text{mod. }p).$$

The question arises, How many such prime functions enter the product on the right? From the derivation of this product, it is seen that only prime functions enter in which the coefficient of the highest power of x is unity. Such prime functions are called *primary prime functions*. Further, there enter in the product only such primary prime functions as are of degree h, or a divisor of h. If d is an arbitrary divisor of h, the number of these prime functions of the dth degree which appear in the product $\Pi P(x)$ may be denoted by Ψ_d. The number of all possible primary prime functions of the dth grade was denoted (Art. 44) by χ_d. It follows then that

$$\Psi_d\leqq\chi_d;$$

and we shall see (Art. 50) that

$$\Psi_d=\chi_d,$$

and that is, there appear in the product $\Pi P(x)$ all possible primary prime functions of the dth degree.

ART. 47. Before determining the number of all possible primary prime functions of a prescribed degree, we must

first find the number of those of the first, second and third degrees, and that is, χ_1, χ_2, χ_3.

A primary prime function of the first degree (mod. p) has the form

$$x+a,$$

where a is a rational integer and is taken (mod. p). It is seen that the functions

$$x,\ x+1,\ x+2,\ \cdots,\ x+p-1$$

form a complete system of incongruent primary prime functions (mod. p) of the first degree, and consequently the number is

$$\chi_1 = p.$$

A primary function of the second degree has the form

$$x^2+ax+b,$$

where a and b are two rational integers determined (mod. p) only. Hence, to have all possible primary prime functions of the second degree, we must give to each of these numbers the values $0, 1, 2, \cdots, p-1$, and subtract from this number the number of functions that are not prime. In all there are p^2 such functions. If one of these functions is not prime, it must be equal to the product of two primary prime functions. Hence, of the p^2 primary functions of the second degree, the number that are not prime is equal to the combination of p elements taken two at a time, allowing repetitions, so that

$$\chi_2 = p^2 - \frac{p(p+1)}{2}, \qquad \text{or} \qquad 2\chi_2 = p(p-1).$$

A primary function of the third degree has the form

$$x^3+ax^2+bx+c;$$

and all the primary functions of the third degree are had by giving to a, b, and c all possible combinations of three equal or different numbers chosen among $0, 1, 2, \cdots, p-1$. We thus have p^3 primary functions. These are

either prime functions or products of a prime function of the first degree with a prime function of the second degree; or products of three primary functions of the first degree. The number of primary prime functions of the third degree is χ_3. The number of the products of a primary prime function of the first degree and of a primary prime function of the second degree is $\chi_1\chi_2$, while the number of the products of three primary prime functions of the first degree is equal to the number of combinations of p elements taken three at a time, allowing repetitions. It follows that

$$p^3=\chi_3+\chi_1\chi_2+\frac{p(p+1)(p+2)}{1\cdot 2\cdot 3},$$

and consequently

$$\chi_3=p^3-\chi_1\chi_2-\frac{p(p+1)(p+2)}{6}$$

$$=p^3-p\cdot\frac{p(p+1)}{2}-\frac{p(p+1)(p+2)}{6};$$

or

$$3\chi_3=p(p^2-1)=p^3-p.$$

ART. **48.** The computation of the number of primary prime functions of any degree h (mod. p) may be made next. The number of primary functions of degree h is p^h, since each of the h coefficients of the primary function may take any of the p numbers which form a complete system of residues (mod. p), and that is, the numbers $0, 1, 2, \cdots, p-1$.

Such a primary function of the hth degree may be either a primary prime function of the hth degree, or a product of a primary prime functions of the first degree, of b primary prime functions of the second degree, of c primary prime functions of the third degree, etc., where $a, b, c, \cdots$ are arbitrary rational integers ($\geqq 0$), which are

subjected only to the condition

$$a+2b+3c+\cdots=h.$$

The question is: In how many different ways is such a representation of a product of a primary prime functions of the first degree, b primary prime functions of the second degree, c primary prime functions of the third degree, etc., possible? There are χ_1 primary prime functions of the first degree, and these may be made into products of a factors in

$$\frac{\chi_1(\chi_1+1)\cdots(\chi_1+a-1)}{a!}$$

different ways. Similarly the χ_2 primary prime functions of the second degree may be combined into

$$\frac{\chi_2(\chi_2+1)\cdots(\chi_2+b-1)}{b!}$$

products of b factors, etc. It is seen that a product of a primary prime functions of the first degree, b primary prime functions of the second degree, etc., may be formed in

$$\frac{\chi_1(\chi_1+1)\cdots(\chi_1+a-1)}{a!}\cdot\frac{\chi_2(\chi_2+1)\cdots(\chi_2+b-1)}{b!}\cdots$$

different ways.

The symbol $\binom{s}{n}$ denotes the well known relation

$$\binom{s}{n}=\frac{s(s-1)\cdots(s-n+1)}{n!},$$

and is used without regard to the nature of s, although n is always a positive integer. The above product may consequently be written

$$(-1)^a\binom{-\chi_1}{a}(-1)^b\binom{-\chi_2}{b}\cdots;$$

and, if a summation is taken over all systems of numbers

$a, b, c, \cdots$, which satisfy the condition

$$a+2b+3c+\cdots=h,$$

the number of primary functions of the degree h is expressed through the formula

$$p^h=\sum_{a,b,c,\cdots}\left\{(-1)^a\binom{-\chi_1}{a}(-1)^b\binom{-\chi_2}{b}\cdots\right\}.$$

If x denotes any variable quantity, it is clear that

$$x^a x^{2b} x^{3c}\cdots=x^h,$$

so that

$$(px)^h=\sum\left\{(-1)^a\binom{-\chi_1}{a}x^a(-1)^b\binom{-\chi_2}{b}x^{2b}\cdots\right\},$$

the summation being taken as above.

Observe that this formula is true for all positive values of h, namely, $h=0, +1, +2, \cdots$, (*ad infinitum*).

If it is assumed that

$$p|x|<1 \qquad \text{or} \qquad |x|<\frac{1}{p},$$

it is clear that

$$\frac{1}{1-px}=\sum_{h=0}^{h=\infty}p^h x^h.$$

It follows at once that

$$\frac{1}{1-px}=\sum_{h=0}^{h=\infty}\left[\sum_{a,b,c,\cdots}\left\{(-1)^a\binom{-\chi_1}{a}x^a(-1)^b\binom{-\chi_2}{b}x^{2b}\cdots\right\}\right].$$

Observe that the double summation may be transformed into a product of an infinite number of single summations, since the infinite series that stands under the double summation is convergent. Further, in the double summation, since h extends over all integral values from zero to infinity, it is seen that $a, b, c, \cdots$, must take all integral values from zero to infinity in each of the single summations, with the result that the formula above may be written

$$\frac{1}{1-px}=\sum\left\{(-1)^a\binom{-\chi_1}{a}x^a\right\}\sum\left\{(-1)^b\binom{-\chi_2}{b}x^{2b}\right\}\cdots.$$

Due to the Binomial Theorem it is evident that

$$(1-x)^{-\chi_1}=\sum_{a=0}^{a=\infty}\left\{(-1)^a\binom{-\chi_1}{a}x^a\right\},$$

$$(1-x^2)^{-\chi_2}=\sum_{b=0}^{b=\infty}\left\{(-1)^b\binom{-\chi_2}{b}x^{2b}\right\},$$

$$(1-x^3)^{-\chi_3}=\sum_{c=0}^{c=\infty}\left\{(-1)^c\binom{-\chi_3}{c}x^{3b}\right\}, \text{ etc.}$$

It follows that

$$\frac{1}{1-px}=(1-x)^{\chi_1}(1-x^2)^{\chi_2}(1-x^3)^{\chi_3}\cdots=\prod_{d=1}^{d=\infty}\{(1-x^d)^{\chi_d}\}.$$

By equating like powers of x on either side of this equation, the positive integers χ_1, χ_2, $\cdots$, (*ad infinitum*) may be calculated.

ART. **49.** From the formula of the preceding article. which is true for

$$|x|<\frac{1}{p},$$

it is further seen that

$$-\log(1-px)=\sum_{d=1}^{d=\infty}\{\chi_d\log(1-x^d)\}.$$

If this expression is differentiated with respect to x, it follows that

$$\frac{p}{1-px}=\sum_{d=1}^{d=\infty}\left\{d\chi_d\frac{x^{d-1}}{1-x^d}\right\};$$

or, if both sides of this equation are multiplied by x,

$$\frac{px}{1-px}=\sum_{d=1}^{d=\infty}\left\{d\chi_d\frac{x^d}{1-x^d}\right\}.$$

Since

$$\frac{px}{1-px}=\sum_{\mu=1}^{\mu=\infty}p^\mu x^\mu \qquad \text{and} \qquad \frac{x^d}{1-x^d}=\sum_{\lambda=1}^{\lambda=\infty}x^{d\lambda},$$

it is seen that

$$\sum_{\mu=1}^{\mu=\infty}p^\mu x^\mu=\sum_{d=1}^{d=\infty}\sum_{\lambda=1}^{\lambda=\infty}d\chi_d x^{d\lambda}.$$

Equating like powers of x in this formula, it is clear that

$$p^h = \sum_d (d\chi_d),$$

where d takes all values in the summation for which $d\lambda = h$; and that is, d goes through all the divisors of h.

Using the well known formula for inversion, it is seen that

$$h\chi_h = \sum_d \{\mu(d) p^{\frac{h}{d}}\},$$

where μ denotes the Möbius coefficients of Art. 45, and d goes through all divisors of h.

ART. **50.** In the formula (Art. 46)

$$x^{p^h} - x \equiv \Pi P(x) \pmod{\mathfrak{p}},$$

observe that the number of primary prime functions of the hth degree, which exist under the product on the right, was denoted by χ_h; while the number of primary prime functions of the degree d (d being any divisor of h), that occur in this product was denoted by Ψ_d. Further, in the above identical congruence, the degree of the highest powers of x must be the same on the right hand and on the left hand sides. It is at once evident that

$$p^h = \sum_d d\Psi_d,$$

where d goes through all divisors of h. It follows as above that

$$h\Psi_h = \sum_d \{\mu(d) p^{\frac{h}{d}}\},$$

where d goes through all divisors of h. From this it results that

$$\Psi_h = \chi_h.$$

It is thus seen that in the product $\Pi P(x)$ all possible primary prime functions enter, whose degree is equal to h, or to a divisor of h; and that is, $x^{p^h} - x$ is congruent to the product of all primary prime functions, whose degree

is equal to h, or to a divisor of h, the congruence being taken (mod. p) or (mod. $\mathfrak{p}$). On the other hand, it was proved (Art. 46) that

$$x^{p^n} - x \equiv \Pi(x - \omega) \pmod{\mathfrak{p}},$$

where ω goes through all incongruent (mod. $\mathfrak{p}$) numbers, whose height is h or a divisor of h. It follows that in the congruence (Vol. I, Art. 198)

$$\Pi P(x) \equiv \Pi(x - \omega) \pmod{\mathfrak{p}},$$

the product on the left is to be taken over all existing primary prime functions, whose degree is h or a divisor of h; while the product on the right is to be taken over all numbers ω, whose height is h or a divisor of h.

EXAMPLE. Derive the analogues of the Fermat and Wilson Theorems, where, instead of taking rational or algebraic integers, the primary prime functions of any degree are taken.

DISTRIBUTION OF IDEALS INTO CLASSES

ART. **51. Equivalent Ideals.** DEFINITION. *Two ideals* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are said to be equivalent, if their quotient is a principal ideal; that is, if there is an integral or fractional number* κ *such that*

$$\frac{\mathfrak{b}}{\mathfrak{a}} = \mathfrak{o}\kappa, \qquad \text{or} \qquad \mathfrak{b} = \kappa\mathfrak{a}.$$

Some authors have defined the equivalence of two ideals somewhat differently, as follows: Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are said to be equivalent, if there is a third ideal $\mathfrak{c}$ such that $\mathfrak{ac}$ and $\mathfrak{bc}$ are principal ideals. This definition is clearly synonymous (coextensive) with the one offered above. For, if $\mathfrak{b}$ is equivalent to $\mathfrak{a}$, then is $\mathfrak{b} = \kappa\mathfrak{a}$; and, if we put

$$\mathfrak{c} = \frac{\mathfrak{o}\alpha}{\mathfrak{a}},$$

where α is an algebraic integer divisible by $\mathfrak{a}$, it is seen that

$$\mathfrak{a}\mathfrak{c} = \mathfrak{o}\alpha \qquad \text{and} \qquad \mathfrak{b}\mathfrak{c} = \mathfrak{o}\kappa\alpha = \mathfrak{o}\beta.$$

If, then, in accordance with the first definition, $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent, it is seen that there exists an ideal $\mathfrak{c}$ such that $\mathfrak{a}\mathfrak{c}$ and $\mathfrak{b}\mathfrak{c}$ are principal ideals. Reciprocally, if there exists an ideal $\mathfrak{c}$ such that

$$\mathfrak{a}\mathfrak{c} = \mathfrak{o}\alpha \qquad \text{and} \qquad \mathfrak{b}\mathfrak{c} = \mathfrak{o}\beta,$$

then is

$$\frac{\mathfrak{b}}{\mathfrak{a}} = \mathfrak{o}\frac{\beta}{\alpha} = \mathfrak{o}\kappa,$$

so that $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent by virtue of the first definition.

ART. 52. **Principal Classes; Reciprocal Classes.** THEOREM. (*1*) *If two ideals* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are equivalent to a third ideal* $\mathfrak{c}$, *they are equivalent to each other.*

For, if

$$\frac{\mathfrak{c}}{\mathfrak{b}} = \mathfrak{o}\lambda \qquad \text{and} \qquad \frac{\mathfrak{c}}{\mathfrak{a}} = \mathfrak{o}\kappa,$$

then

$$\frac{\mathfrak{b}}{\mathfrak{a}} = \mathfrak{o}\frac{\kappa}{\lambda} = \mathfrak{o}\mu.$$

To the above theorem may be added the two which follow, and which may be proved readily: (*2*) *Every ideal is equivalent to itself.* (*3*) *If an ideal* $\mathfrak{a}$ *is equivalent to an ideal* $\mathfrak{b}$, *then also* $\mathfrak{b}$ *is equivalent to* $\mathfrak{a}$.

On the truth of these theorems rests the possibility of the distribution of all ideals of a fixed realm into classes of equivalent ideals. For, if a distribution into classes is made such that two equivalent ideals fall into the same class, while two ideals that are not equivalent fall into different classes, then two different classes in virtue of the theorems above have no ideals in common.

If $\mathfrak{a}$ is an ideal belonging to one class, it may be taken as the representative of this class; or, any other ideal

equivalent to $\mathfrak{a}$ may be taken as the representative of this class. All ideals belonging to the class, of which $\mathfrak{a}$ is a representative, must have the form $\mathfrak{a}\xi$, where ξ is an algebraic number.

Reciprocally, since all ideals of the form $\mathfrak{a}\xi$ are equivalent to $\mathfrak{a}$, it is seen that they must belong to the same class to which $\mathfrak{a}$ belongs. This class may be denoted by A. It is clear that all principal ideals belong to a class. This class may be called the *principal class*, and may be denoted by U.

If $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals, and if A and B are the two classes to which they belong, then all products which are had if an ideal of the class A is multiplied by an ideal of the class B, are equivalent to the product $\mathfrak{ab}$. For, all such products have the form

$$\mathfrak{a}\xi \cdot \mathfrak{b}\eta = \mathfrak{ab}\xi\eta = \mathfrak{ab}\zeta,$$

and consequently belong to the class represented by $\mathfrak{ab}$.

Reciprocally, all the ideals that are equivalent to the product $\mathfrak{ab}$ are had, if every ideal of the class A is multiplied by every ideal of the class B. This class C is called the *product* of the two classes A and B. Clearly, the class $C = AB$ has the form $\mathfrak{ab}\zeta$, where ζ is an arbitrary algebraic number.

It follows that

$$AB = BA.$$

Similarly, it is seen that

$$A(BC) = (AB)C,$$

where A, B and C are three classes that are *not* necessarily different. Accordingly, in the above definition, the parentheses may be omitted, so that

$$ABC = A(BC) = (AB)C.$$

It follows then that the commutative and the associative principles hold for the products of classes.

From the associative principle follow the laws of exponents, so that

$$AA = A^2, \qquad AAA = A^3, \qquad AAAA = A^4, \text{ etc.}$$

From the associative principle, observe *first* that

$$A^r A^s = A^{r+s}$$

for the case that r and s are two positive integers, different from zero. Note *next* that

$$UA = A \qquad \text{or} \qquad A^0 = A \div A = U.$$

Accordingly, if $s > 0$, we have

$$UA^s = A^s \qquad \text{or} \qquad A^0 A^s = A^s.$$

It is seen further that the product of two principal classes is a principal class. For, we have

$$A^0 A^0 = UU = U = A^0;$$

and consequently, the formula

$$A^r A^s = A^{r+s}$$

is also true if one or both of the indices is zero.

If A is a class, and if the ideal $\mathfrak{a}$ is its representative, then all ideals of the class A have the form $\mathfrak{a}\xi$. It is seen also that all ideals of the form

$$(\mathfrak{a}\xi)^{-1} = \mathfrak{a}^{-1}\xi^{-1}$$

are equivalent to one another, being all equivalent to $\mathfrak{a}^{-1}$. If we take the reciprocal ideals (Art. 8) to all the ideals of a class A, it is evident that they form a class which may be denoted by A^{-1}.

Further, since

$$\mathfrak{a}\xi\mathfrak{a}^{-1}\xi^{-1} = \mathfrak{o},$$

it follows that

$$AA^{-1} = U.$$

It is thus proved that to every class A there corresponds a class B, such that

$$AB = U.$$

It may be proved that there is only *one* class B which satisfies the condition

$$AB = U.$$

For, suppose that C is also a class such that

$$AC = U.$$

It follows that

$$ABC = (AB)C = UC = C,$$

and also that

$$ABC = (AC)B = UB = B;$$

and consequently,

$$B = C.$$

The class B which is uniquely determined through the condition

$$AB = U,$$

is denoted by A^{-1} and is called the *reciprocal* class of the class A. It follows that the reciprocal class A^{-1} is the class which, compounded with the class A, gives the principal class.

It follows further that

$$A^n(A^n)^{-1} = U,$$
$$A^n(A^{-1})^n = (AA^{-1})^n = U^n = U,$$

so that

$$A^{-n} = (A^n)^{-1} = (A^{-1})^n.$$

Having thus defined classes with negative exponents, it is clear that the formulas already derived for positive values of r and s, namely,

$$A^rA^s = A^{r+s},$$
$$A^rB^r = (AB)^r,$$

are true also if one or both of the integers r and s are less than or equal to 0.

ART. 53. **The Number of Classes Is Finite.** Before giving a proof of this statement, it is necessary to introduce a lemma.

Denote as usual by $|x+iy|$ the quantity $+\sqrt{x^2+y^2}$. Further, suppose that Ω is an algebraic realm of rationality of the nth degree, and let $\omega_1, \omega_2, \cdots, \omega_n$ form a basis of $\mathfrak{o}$ in Ω. Let the quantities conjugate to ω_ν, be $\omega_\nu(=\omega_\nu')$, $\omega_\nu'', \cdots, \omega_\nu^{(n)} (\nu = 1, 2, \cdots, n)$. Take rational integers $h_1, h_2, \cdots, h_n$, which are less than or equal to a fixed rational integer k, and write

$$\alpha = h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n.$$

Let the quantities conjugate with and including α be $\alpha', \alpha'', \cdots, \alpha^{(n)}$. If r is one of the numbers $1, 2, \cdots, n$, it follows that

$$\alpha^{(r)} = h_1\omega_1^{(r)} + h_2\omega_2^{(r)} + \cdots + h_n\omega_n^{(r)}.$$

Consequently,

$$|\alpha^{(r)}| \leqq |h_1|\,|\omega_1^{(r)}| + |h_2|\,|\omega_2^{(r)}| + \cdots + |h_n|\,|\omega_n^{(r)}|.$$

Since $h_1, h_2, \cdots, h_n$ are all less than or equal to k, we have

$$|\alpha^{(r)}| \leqq k\{|\omega_1^{(r)}| + |\omega_2^{(r)}| + \cdots + |\omega_n^{(r)}|\}.$$

In this expression give r the values $1, 2, \cdots, n$ and multiply the resulting expressions together. It follows that

$$\prod_{r=1}^{r=n} |\alpha^{(r)}| \leqq k^n M,$$

where

$$M = \prod_{r=1}^{r=n} \{|\omega_1^{(r)}| + |\omega_2^{(r)}| + \cdots + |\omega_n^{(r)}|\};$$

and, since

$$\prod_{r=1}^{r=n} |\alpha^{(r)}| = \left|\prod_{r=1}^{r=n} \alpha^{(r)}\right| = |N(\alpha)|,$$

it is evident that

$$|N(\alpha)| \leqq k^n M.$$

The following lemma may be proved. LEMMA. *If* $\mathfrak{a}$ *is an ideal of the nth order in a realm of the nth degree, there*

is always an integer which is divisible by $\mathfrak{a}$ *and whose norm is* $\leqq(\mathfrak{o}, \mathfrak{a})M$.

Since $\mathfrak{o}$ and $\mathfrak{a}$ are both finite moduls, $(\mathfrak{o}, \mathfrak{a})$ is a finite positive rational integer. Let the greatest integer in $\sqrt[n]{(\mathfrak{o}, \mathfrak{a})}$ be k, so that

$$k \leqq \sqrt[n]{(\mathfrak{o}, \mathfrak{a})} < k+1 \qquad \text{or} \qquad k^n \leqq (\mathfrak{o}, \mathfrak{a}) < (k+1)^n.$$

Again, consider the algebraic integers of Ω of the form

$$\sigma = h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n.$$

If in this expression the integers $h_1, h_2, \cdots, h_n$ take the values $0, 1, 2, \cdots, k$, there are $(k+1)^n$ different integers σ of Ω. Next, consider these $(k+1)^n$ integers (mod. $\mathfrak{a}$). The number of all incongruent (mod. $\mathfrak{a}$) numbers of the form (Art. 19)

$$h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n$$

is $(\mathfrak{o}, \mathfrak{a})$.

Further,

$$(\mathfrak{o}, \mathfrak{a}) < (k+1)^n.$$

It follows that of the $(k+1)^n$ numbers which are had from the form

$$\sigma = h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n,$$

when in this form the values $0, 1, 2, \cdots, k$ are given to $h_1, h_2, \cdots, h_n$, there are at least two different, which are congruent (mod. $\mathfrak{a}$). Hence, a necessary congruence is

$$b_1\omega_1 + b_2\omega_2 + \cdots + b_n\omega_n \equiv c_1\omega_1 + c_2\omega_2 + \cdots + c_n\omega_n \pmod{\mathfrak{a}},$$

where $b_1, b_2, \cdots, b_n, c_1, c_2, \cdots, c_n$ are rational integers which lie between 0 and k, and where *all* the differences $b_\nu - c_\nu$ $(\nu = 1, 2, 3, \cdots, n)$ do not vanish. If then we write

$$b_\nu - c_\nu = a_\nu \qquad (\nu = 1, 2, \cdots, n)$$

the a's are not all zero. In absolute value they are all less than or equal to k. It is further seen that

$$a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n$$

is divisible by $\mathfrak{a}$. Denote this number by α. It follows

from above that

$$|N(\alpha)| \leqq k^n M;$$

and since

$$k^n \leqq (\mathfrak{o}, \mathfrak{a}),$$

it is evident that

$$|N(\alpha)| \leqq (\mathfrak{o}, \mathfrak{a}) M.$$

It is thus proved that in every ideal $\mathfrak{a}$ there is a number α such that

$$|N(\alpha)| \leqq (\mathfrak{o}, \mathfrak{a}) M.$$

ART. **54.** Suppose that $\mathfrak{b}$ is an integral ideal of the realm Ω, and consequently (Art. 16),

$$(\mathfrak{o}, \mathfrak{b}) = N(\mathfrak{b}).$$

Due to the lemma of the preceding article, there is a number β divisible by $\mathfrak{b}$, such that

$$|N(\beta)| \leqq N(\mathfrak{b}) M.$$

Since β is divisible by $\mathfrak{b}$, we have

$$\mathfrak{o}\beta > \mathfrak{b},$$

and consequently $\frac{\mathfrak{o}\beta}{\mathfrak{b}}$ is an integral ideal, equal to $\mathfrak{a}$, say;

or

$$\mathfrak{o}\beta = \mathfrak{a}\mathfrak{b}.$$

It follows that

$$|N(\mathfrak{o}\beta)| = N(\mathfrak{a}) N(\mathfrak{b}) \leqq M N(\mathfrak{b}),$$

or

$$N(\mathfrak{a}) \leqq M.$$

If we consider any class A, its reciprocal or inverse is A^{-1}. As an arbitrary ideal may by multiplication with a rational integer be changed into an integral ideal (Vol. I, Art. 93), there is in every class at least *one* integral ideal. There is consequently in the class A^{-1} an integral ideal which may be denoted by $\mathfrak{b}$. If β is a number divisible by $\mathfrak{b}$; and if further

$$\frac{\mathfrak{o}\beta}{\mathfrak{b}} = \mathfrak{a},$$

then the ideal $\mathfrak{a}$ belongs to the class which is the inverse of the class A^{-1}; that is, $\mathfrak{a}$ belongs to the class A, since the ideal $\mathfrak{a}$ compounded with the ideal $\mathfrak{b}$ offers a principal ideal.

We saw that

$$N(\mathfrak{a}) \leqq M.$$

Since the class A, with which we started is perfectly arbitrary, it is shown that in every arbitrary class A there is an ideal $\mathfrak{a}$ which is integral and which satisfies the condition

$$N(\mathfrak{a}) \leqq M.$$

Further, since M is a finite real number, there are a finite number of rational integers g which are less than or equal to M.

There is only a finite number of integral ideals $\mathfrak{a}$, whose norm equal g (Arts. 19, 25), and this, combined with the fact that

$$N(\mathfrak{a}) \leqq M$$

offers the following important theorem: *The number of classes in a finite realm of rationality is finite.* (See Art. 158.)

The above proof is due to Kronecker (" De unitatibus complexis," § 6).

ART. **55. Number of Ideal-Classes.** The determination of the number of classes of ideals in general has not been done. In special realms the number is known; for example, in the quadratic, the cubic, and the realms that are determined through the roots of unity. By virtue of the theorem, however, that the number of classes is finite, many important consequences may be drawn. In the sequel the number of classes is denoted by h. Let

$$A_1, A_2, \cdots, A_h$$

be these different classes. If A is any one of them, then

$$AA_1,\ AA_2,\ \cdots,\ AA_h$$

form again h classes which are different from one another. For, if

$$AA_r = AA_s,$$

it would follow that

$$A^{-1}AA_r = A^{-1}AA_s \qquad \text{or} \qquad A_r = A_s,$$

which is *not* true. Since $AA_1,\ AA_2,\ \cdots,\ AA_h$ are, neglecting the sequence, the same classes as $A_1,\ A_2,\ \cdots,\ A_h$, it is seen that

$$A^h A_1 A_2 \cdots A_h = A_1 A_2 \cdots A_h,$$

or

$$A^h A_1 A_2 \cdots A_h [A_1 A_2 \cdots A_h]^{-1} = A_1 A_2 \cdots A_h [A_1 A_2 \cdots A_h]^{-1},$$

and finally,

$$A^h = U.$$

The following theorem admits immediate proof. THEOREM. *If h is the number of classes of ideals in a given realm, the h power of every ideal is a principal ideal.*

For, if $\mathfrak{a}$ is an ideal which belongs to the class A, then $\mathfrak{a}^h$ belongs to the class A^h; and that is, the principal class U. It follows that $\mathfrak{a}^h$ is a principal ideal.

Suppose further that

$$\mathfrak{a}^h = \mathfrak{o}\alpha,$$

where α is a number of the fixed realm Ω; and let ξ be any integer that is divisible by $\mathfrak{a}$. It follows that ξ^h is divisible by $\mathfrak{a}^h$; and that is, by $\mathfrak{o}\alpha$. Consequently, $\frac{\xi^h}{\alpha}$ is an algebraic integer. Since the h root of an algebraic integer is an algebraic integer, it follows that $\xi / \sqrt[h]{\alpha}$ is an algebraic integer. It is thus seen that every algebraic integer ξ that is divisible by the ideal $\mathfrak{a}$, is divisible by $\sqrt[h]{\alpha}$.

Reciprocally, suppose that ξ is divisible by $\sqrt[h]{\alpha}$, so that ξ^h is divisible by α, then, since

$$\mathfrak{o}\alpha = \mathfrak{a}^h,$$

it follows that ξ^h is divisible by $\mathfrak{a}^h$, and consequently ξ by $\mathfrak{a}$.

It is evident that to every ideal $\mathfrak{a}$ there corresponds a number $\sqrt[h]{\alpha}$, which, although itself not divisible by the ideal $\mathfrak{a}$, has the property that all numbers divisible by $\mathfrak{a}$ are the same as all the numbers that are divisible by $\sqrt[h]{\alpha}$. This number $\sqrt[h]{\alpha}$ does *not* in general belong to the fixed realm Ω. It may be called an *ideal number* of Ω.

ART. **56.** The following important theorem may be proved. THEOREM. *If α and β are two arbitrary algebraic numbers, there is always a third algebraic number δ, such that (1) α and β are both divisible by δ; and (2) there are two algebraic integers ξ and η, such that*

$$\delta = \alpha\xi + \beta\eta.$$

If one of the numbers α or β is zero, the theorem offers nothing new. Without restricting the generality, it may consequently be assumed that α and β are both different from zero.

It is always possible (Vol. I, Art. 51) to determine an algebraic realm to which both α and β belong. If this realm is $\Re(\theta)$, it is seen that both α and β may be expressed rationally through the algebraic number θ. Let $\mathfrak{o}$ be the order-modul formed of all the algebraic integers of this realm, and let

$$\mathfrak{d} = \mathfrak{o}\alpha + \mathfrak{o}\beta.$$

We then have

$$\mathfrak{o}\alpha > \mathfrak{d} \qquad \text{and} \qquad \mathfrak{o}\beta > \mathfrak{d};$$

and consequently $\frac{\mathfrak{o}\alpha}{\mathfrak{d}}$ and $\frac{\mathfrak{o}\beta}{\mathfrak{d}}$ are integral ideals which may be denoted by $\mathfrak{a}$ and by $\mathfrak{b}$, respectively.

If the number of classes of the realm $\Re(\theta)$ is denoted by h, it follows from above that

$$\mathfrak{b}^h = \mathfrak{o}\delta_1,$$

where δ_1 is a number of $\Re(\theta)$. It follows also that

$$(\mathfrak{o}\alpha)^h = \mathfrak{a}^h\mathfrak{b}^h = \mathfrak{a}^h\mathfrak{o}\delta_1 = \mathfrak{a}^h\delta_1$$

and

$$(\mathfrak{o}\beta)^h = \mathfrak{b}^h\mathfrak{b}^h = \mathfrak{b}^h\mathfrak{o}\delta_1 = \mathfrak{b}^h\delta_1.$$

It is thus seen that α^h and β^h are both divisible by δ_1 and consequently we may write

$$\frac{\alpha^h}{\delta_1} = \alpha_1, \qquad \frac{\beta^h}{\delta_1} = \beta_1,$$

where α_1 and β_1 are algebraic integers.

We thus have

$$\alpha^h = \alpha_1\delta_1 \qquad \text{and} \qquad \beta^h = \beta_1\delta_1;$$

or

$$\mathfrak{o}\alpha^h = \mathfrak{o}\alpha_1\delta_1 \qquad \text{and} \qquad \mathfrak{o}\beta^h = \mathfrak{o}\beta_1\delta_1.$$

Or, on the other hand, since

$$\mathfrak{o}\alpha^h = \mathfrak{a}^h\delta_1 \qquad \text{and} \qquad \mathfrak{o}\beta^h = \mathfrak{b}^h\delta_1,$$

we must have

$$\mathfrak{a}^h = \mathfrak{o}\alpha_1 \qquad \text{and} \qquad \mathfrak{b}^h = \mathfrak{o}\beta_1.$$

Since $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime, $\mathfrak{a}^h$ and $\mathfrak{b}^h$ must also be relatively prime, so that α_1 and β_1 are relatively prime. We may therefore (Art. 18) determine two algebraic integers ξ_1 and η_1, such that

$$\alpha_1\xi_1 + \beta_1\eta_1 = 1.$$

If this equation is multiplied by δ_1, we find that

$$\delta_1 = \alpha_1\delta_1\xi_1 + \beta_1\delta_1\eta_1 = \alpha^h\xi_1 + \beta^h\eta_1.$$

If, further, we put $\delta_1 = \delta^h$, we have

$$\delta^h = \alpha\cdot\alpha^{h-1}\xi_1 + \beta\cdot\beta^{h-1}\eta_1.$$

It was seen above that α^h was divisible by δ_1 or by δ^h, so that α is divisible by δ, and consequently α^{h-1} by δ^{h-1},

and similarly, β^{h-1} by δ^{h-1}. If then we put

$$\alpha^{h-1}\xi_1 = \delta^{h-1}\xi, \qquad \beta^{h-1}\eta_1 = \delta^{h-1}\eta,$$

we see that ξ and η are algebraic integers, which however, do *not* necessarily belong to the realm $\Re(\theta)$. It follows that

$$\delta^h = \delta^{h-1}\alpha\xi + \delta^{h-1}\beta\eta,$$

or

$$\delta = \alpha\xi + \beta\eta.$$

It has thus been seen that both α and β are divisible by δ, which proves the theorem stated at the beginning of this article.

ART. **57.** If it is assumed that there is another number δ' which has the properties: (1) that α and β are both divisible by δ'; and (2) that two algebraic integers ξ' and η' may be determined such that

$$\delta' = \alpha\xi' + \beta\eta',$$

it would follow that

$$\frac{\delta}{\delta'} = \frac{\alpha}{\delta'}\xi + \frac{\beta}{\delta'}\eta \qquad \text{and} \qquad \frac{\delta'}{\delta} = \frac{\alpha}{\delta}\xi' + \frac{\beta}{\delta}\eta'.$$

Since ξ, η, ξ', η', $\frac{\alpha}{\delta'}$, $\frac{\alpha}{\delta}$, $\frac{\beta}{\delta'}$, $\frac{\beta}{\delta}$ are all algebraic integers, it is clear that $\frac{\delta}{\delta'}$ and $\frac{\delta'}{\delta}$ are algebraic integers; or δ and δ' are associated numbers (Vol. I, Art. 91). It is thus seen that the number δ is not uniquely determined (but only as to a multiplicative algebraic unit) through the two properties (1) and (2).

If δ' is any common divisor of α and β so that $\frac{\alpha}{\delta'}$ and $\frac{\beta}{\delta'}$ are algebraic integers, it is seen that $\frac{\delta}{\delta'}$ is an algebraic integer, or δ is divisible by δ'. Hence the number δ, determined by the two properties given above, is divisible

by every common divisor δ' of α and β. It is therefore appropriate to say that δ, the number determined through these two properties, is the *greatest common divisor* of the two algebraic numbers α and β.

It has thus been proved, and this is the key to the whole theory of ideals, that every two algebraic numbers have a greatest common divisor δ which is characterized by the two properties (1) and (2).

It must be noted that the greatest common divisor δ of two algebraic numbers α and β does not belong to the same realm of rationality *in general* as do α and β.

ART. **58.** If $\tau, \tau^{(1)}, \cdots, \tau^{(n-1)}$ are conjugate quantities of a realm $\Re(\theta)$, it is seen that $N(\tau) = \tau \cdot \tau^{(1)} \cdots \tau^{(n-1)} = r$, where r is a rational number. Further $\tau^{(1)}\tau^{(2)} \cdots \tau^{(n-1)} = \frac{r}{\tau}$ is a number of $\Re(\theta)$, as is also $\tau^{(1)} + \tau^{(2)} + \cdots + \tau^{(n-1)} = a - \tau$, where a is a rational number.

If τ is any integer of an ideal, then is also $N(\tau)$. For $\tau^{(1)}$ satisfies the same algebraic equation as does τ and is accordingly an integer, as is the product $\tau^{(1)}\tau^{(2)} \cdots \tau^{(n-1)}$. And this product from above is an integer of $\Re(\theta)$. Hence in every ideal there are to be found rational integers.

In Art. 19 it was seen that the norm of an integral ideal is divisible by the ideal.

THEOREM. *Every rational integer has only a finite number of ideal divisors.* For, if a is divisible by $\mathfrak{a} = (\alpha_1, \alpha_2, \cdots, \alpha_n)$, it may be added as an element of $\mathfrak{a}$, so that $\mathfrak{a} = (\alpha_1, \alpha_2, \cdots, \alpha_n, a)$.

If $\omega_1, \omega_2, \cdots, \omega_n$ form a basis of all integers of $\Re(\theta)$, it is seen that

$$\alpha_i = g_{1i}\omega_1 + g_{2i}\omega_2 + \cdots + g_{ni}\omega_n \quad (i = 1, 2, \cdots, n).$$

Since the rational integers g_{ki} $(k, i = 1, 2, \cdots, n)$ may be

reduced (mod. a), there can be only a finite number of different elements α_i, and consequently also a finite number of ideals $\mathfrak{a}$. Similarly, it follows at once that *any ideal* $\mathfrak{i}$ *has only a finite number of ideal divisors.* (See Art. 25.) *The only ideal that contains 1 as an element is the order-modul* $\mathfrak{o}$ *of the realm* $\Re(\theta)$. For each of the integers g_{ki} in this case may be replaced by 1 or 0.

This may also be proved as follows:

If $[1]>\mathfrak{i}$, then also is $\mathfrak{o}[1]>\mathfrak{i}$, and that is $\mathfrak{o}>\mathfrak{i}$. And since $\mathfrak{i}>\mathfrak{o}$, it follows that

$$\mathfrak{o}=\mathfrak{i}.$$

EXAMPLE. If $\mathfrak{a}$ is any ideal, it is always possible to find an integer α of $\mathfrak{a}$ such that $\alpha/\mathfrak{a}$ is prime to a prime ideal $\mathfrak{p}$. For otherwise all numbers of $\mathfrak{a}$ would be divisible by $\mathfrak{ap}$, which is not true. Show that the theorem is at once applicable, if we take any ideal $\mathfrak{b}$ instead of $\mathfrak{p}$.

ART. **59.** In Art. 36 it was seen that the degree f of the prime ideal $\mathfrak{p}$ is the least number, such that for every integer γ in $\mathfrak{o}$ there exists the congruence

$$\gamma^{p^f}\equiv\gamma \pmod{\mathfrak{p}}. \tag{1}$$

Let $\gamma_1, \gamma_2, \cdots, \gamma_n$ be any basis of $\mathfrak{o}$. All these elements cannot be divisible by $\mathfrak{p}$, otherwise $\mathfrak{o}$ would be divisible by $\mathfrak{p}$. Let γ_1 be an element that is *not* divisible by $\mathfrak{p}$; then by joining with this element a second basal element, γ_2 say, and then a third, etc., we finally derive a certain number of elements $\gamma_1, \gamma_2, \cdots, \gamma_k$ that are (mod. $\mathfrak{p}$) *independent;* and that is, they are such that the congruence

$$r_1\gamma_1+r_2\gamma_2+\cdots+r_k\gamma_k\equiv 0 \pmod{\mathfrak{p}} \tag{2}$$

can only exist, when the rational integers $r_1, r_2, \cdots, r_k$ are all divisible by p, where p is the rational prime integer that is divisible by $\mathfrak{p}$. It is asserted that *this number* k *of basal elements of* $\mathfrak{o}$ *which are independent of one another*

(mod. $\mathfrak{p}$*) is the same as* f*, where* f *is the degree of the prime ideal* $\mathfrak{p}$.

For, if γ_m is any other basal element, it follows that

$$r_m\gamma_m+r_1\gamma_1+r_2\gamma_2+\cdots+r_k\gamma_k\equiv 0 \pmod{\mathfrak{p}}, \tag{3}$$

where r_m is a rational integer that is relatively prime to p.

It follows further that two other rational integers s and q may be found such that

$$sr_m+pq=1;$$

and this combined with (3) shows that

$$\gamma_m\equiv s_1\gamma_1+s_2\gamma_2+\cdots+s_k\gamma_k,$$

where s_i $(i=1, 2, \cdots, k)$ are rational integers. As this is true of all other elements γ_i that do not appear in equation (2), it is seen that any integer τ of the realm may be expressed in the form

$$\tau\equiv a_1\gamma_1+a_2\gamma_2+\cdots+a_k\gamma_k \pmod{\mathfrak{p}}, \tag{4}$$

and any other integer σ may be expressed through

$$\sigma\equiv b_1\gamma_1+b_2\gamma_2+\cdots+b_k\gamma_k \pmod{\mathfrak{p}}.$$

It is further seen that $\sigma\equiv\tau \pmod{\mathfrak{p}}$ only when the difference

$$(a_1-b_1)\gamma_1+(a_2-b_2)\gamma_2+\cdots+(a_k-b_k)\gamma_k\equiv 0 \pmod{\mathfrak{p}}.$$

And this, due to the independence of the elements $\gamma_1, \gamma_2, \cdots, \gamma_k$, can only be when $a_i=b_i$ $(i=1, 2, \cdots, k)$, since the a's and b's are reduced (mod. p).

Hence, by letting each of the integers $a_1, a_2, \cdots, a_k$ go through a complete set of incongruent (mod. p) integers, we derive a complete set of incongruent (mod. $\mathfrak{p}$) integers of $\mathfrak{o}$. The number of these being

$$p^k=(\mathfrak{o}, \mathfrak{p})=N(\mathfrak{p})=p^f,$$

shows that $k=f$.

ART. **60.** Another meaning of the degree f of the prime ideal $\mathfrak{p}$ is given by Hensel (*Crelle's Journal*, Vol. 113, p. 68): Form the matrix

$$\begin{pmatrix} \omega_1, & \omega_2, & \cdots, & \omega_n \\ \omega_1^p, & \omega_2^p, & \cdots, & \omega_n^p \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ \omega_1^{p^\lambda}, & \omega_2^{p^\lambda}, & \cdots, & \omega_n^{p^\lambda} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \end{pmatrix},$$

where $\omega_1, \omega_2, \cdots, \omega_n$ are a basis of $\mathfrak{o}$. Since $\gamma^{p^f} \equiv \gamma \pmod{\mathfrak{p}}$ for every integer of $\mathfrak{o}$, it is seen, when this matrix is considered (mod. $\mathfrak{p}$), that there are only f consecutive rows that are different from one another. And from this it follows that all determinants of the order $f+1$ or higher are zero. On the other hand, it may be shown that at least one of the determinants of the fth order is different from zero (mod. $\mathfrak{p}$). For, were all the determinants of the matrix

$$\begin{pmatrix} \omega_1, & \omega_2, & \cdots, & \omega_n \\ \omega_1^p, & \omega_2^p, & \cdots, & \omega_n^p \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ \omega_1^{p^{f-1}}, & \omega_2^{p^{f-1}}, & \cdots, & \omega_n^{p^{f-1}} \end{pmatrix}$$

congruent to 0 (mod. $\mathfrak{p}$), it would be possible (Vol. I, Art. 56) to find f algebraic integers $\gamma_0, \gamma_1, \cdots, \gamma_{f-1}$, such that for all n integers $\omega_1, \omega_2, \cdots, \omega_n$ the congruences

$$(1) \quad \gamma_0\omega_i + \gamma_1\omega_i^p + \cdots + \gamma_{f-1}\omega_i^{p^{f-1}} \equiv 0 \pmod{\mathfrak{p}} \quad (i = 1, 2, \cdots, n)$$

exist.

Let $\tau_0, \tau_1, \cdots, \tau_{f-1}$ be any algebraic integers defined through the congruences (mod. p)

$$\begin{cases} \tau_0 \equiv a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n, \\ \tau_1 \equiv a_1\omega_1^p + a_2\omega_2^p + \cdots + a_n\omega_n^p, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \tau_{f-1} \equiv a_1\omega_1^{p^{f-1}} + a_2\omega_2^{p^{f-1}} + \cdots + a_n\omega_n^{p^{f-1}}, \end{cases}$$

in which the a's are rational integers.

If these congruences are multiplied respectively by

$\gamma_0, \gamma_1, \cdots, \gamma_{f-1}$ and added, we have

$$\gamma_0\tau_0+\gamma_1\tau_1+\cdots+\gamma_{f-1}\tau_{f-1}\equiv 0 \pmod{\mathfrak{p}}. \tag{2}$$

In this expression write instead of the arbitrary integers $\tau_0, \tau_1, \cdots, \tau_{f-1}$, the integers $\sigma_0^h, \sigma_1^h, \cdots, \sigma_{f-1}^h$ and let h take respectively the values $0, 1, \cdots, f-1$. In this way are had the f congruences (mod. $\mathfrak{p}$) that follow:

$$\begin{aligned}
\gamma_0+\gamma_1+\cdots+\gamma_{f-1}&\equiv 0,\\
\gamma_0\sigma_0+\gamma_1\sigma_1+\cdots+\gamma_{f-1}\sigma_{f-1}&\equiv 0,\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots&\\
\gamma_0\sigma_0^{f-1}+\gamma_1\sigma_1^{f-1}+\cdots+\gamma_{f-1}\sigma_{f-1}^{f-1}&\equiv 0.
\end{aligned}$$

These congruences can only exist if their determinant $\equiv 0$ (mod. $\mathfrak{p}$); and that is, if

$$\begin{vmatrix} 1, & 1, & \cdots, & 1 \\ \sigma_0, & \sigma_1, & \cdots, & \sigma_{f-1} \\ \cdots & \cdots & \cdots & \cdots \\ \sigma_0^{f-1}, & \sigma_1^{f-1}, & \cdots, & \sigma_{f-1}^{f-1} \end{vmatrix} = \prod_{i>j}(\sigma_i-\sigma_j)$$

is divisible by $\mathfrak{p}$.

As the σ_i are arbitrary integers, they may be taken so that none of their differences is divisible by $\mathfrak{p}$. And this precludes the original supposition. We may accordingly for simplicity suppose that the basal elements $\omega_1, \omega_2, \cdots, \omega_n$ have been so chosen that

$$\Delta = \begin{vmatrix} \omega_1, & \omega_2, & \cdots, & \omega_f \\ \omega_1^p, & \omega_2^p, & \cdots, & \omega_f^p \\ \cdots & \cdots & \cdots & \cdots \\ \omega_1^{p^{f-1}}, & \omega_2^{p^{f-1}}, & \cdots, & \omega_f^{p^{f-1}} \end{vmatrix} \not\equiv 0 \pmod{\mathfrak{p}}.$$

It is then seen that the f elements $\omega_1, \omega_2, \cdots, \omega_f$ form (mod. $\mathfrak{p}$) a fundamental system such that every integer γ of $\mathfrak{o}$ may be expressed (mod. $\mathfrak{p}$) in one and only way in the form

$$\begin{aligned}
\gamma &\equiv g_1\omega_1+g_2\omega_2+\cdots+g_f\omega_f,\\
\gamma^p &\equiv g_1\omega_1^p+g_2\omega_2^p+\cdots+g_f\omega_f^p,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
\gamma^{p^{f-1}} &\equiv g_1\omega_1^{p^{f-1}}+g_2\omega_2^{p^{f-1}}+\cdots+g_f\omega_f^{p^{f-1}} \pmod{\mathfrak{p}}.
\end{aligned}$$

For, since the determinant of these congruences is not divisible by $\mathfrak{p}$, the g's are uniquely determined (mod. $\mathfrak{p}$). Further, if the above congruences are each raised to the p power, it is seen that $g_1^p, g_2^p, \cdots, g_f^p$ satisfy the same congruences as do $g_1, g_2, \cdots, g_f$ (mod. $\mathfrak{p}$). And accordingly (Art. 41) the g's are congruent to rational integers (mod. p). We have thus all the incongruent (mod. $\mathfrak{p}$) integers of $\mathfrak{o}$, if in the form

$$g_1\omega_1+g_2\omega_2+\cdots+g_f\omega_f$$

we allow the integers $g_1, g_2, \cdots, g_f$ to take respectively the values $0, 1, \cdots, p-1$.

With this is proved again the theorem: *The number of incongruent (mod.* $\mathfrak{p}$*) integers of* $\mathfrak{o}$ *is* p^f, *where* f *is the degree of* $\mathfrak{p}$.

ART. **61.** In Art. 44 it was proved that there exist integers γ of $\mathfrak{o}$ that *belong* to p^f-1; and that is, γ must be raised to the power p^f-1 before the congruence

$$\gamma^{p^f-1}\equiv 1 \pmod{\mathfrak{p}}$$

is satisfied. Such numbers were called *primitive numbers* (Vol. I, Art. 224). There are $\varphi(p^f-1)$ such numbers in $\mathfrak{o}$, as may be proved precisely as in the case for rational integers.

It was proved in Art. 43 that these primitive integers are the roots of $\dfrac{\varphi(p^f-1)}{f}$ irreducible functions, each of the fth degree. Accordingly, every primitive number of a fixed realm satisfies (mod. p) an irreducible equation of the fth degree.

Let $P(x)$ be any arbitrary irreducible (mod. p) function with rational integral coefficients, m its degree; and let ρ be any root of the congruence

$$P(x)=a_0+a_1x+a_2x^2+\cdots+a_mx^m\equiv 0 \pmod{\mathfrak{p}};$$

and that is, let ρ be an integer of the fixed realm such that $P(\rho)$ is an integer of the ideal $\mathfrak{p}$.

Observe next (see Vol. I, Art. 195), if $F(x)$ is any other integral function with integral coefficients, that the number-congruence

$$F(\rho)\equiv 0 \pmod{\mathfrak{p}}$$

has the same significance [1] as the functional congruence

$$F(x)\equiv 0 \ [\text{modd. } p,\ P(x)], \tag{1}$$

and *vice versa*.

For, from the latter congruence, it follows that

$$F(x)=p\varphi(x)+P(x)\Psi(x),$$

where $\varphi(x)$ and $\Psi(x)$ are integral functions with integral coefficients. And from this it is seen that

$$F(\rho)\equiv 0 \pmod{\mathfrak{p}}.$$

On the other hand, if this last congruence exists, then $F(x)$ must be congruent to zero [modd. p, $P(x)$]. Otherwise $F(x)$ and $P(x)$ would be relatively prime (mod. p). In this case there exist two functions with integral coefficients $\varphi_1(x)$ and $\varphi_2(x)$ such that

$$F(x)\varphi_1(x)+P(x)\varphi_2(x)\equiv 1 \pmod{p};$$

and since $F(\rho)$ and $P(\rho)$ are both congruent to zero (mod. $\mathfrak{p}$), it would follow that

$$0\equiv 1 \pmod{\mathfrak{p}}.$$

Further it is seen from (1) that a congruence, in which the degree of $F(x)$ is less than that of $P(x)$, cannot exist unless

$$F(x)\equiv 0 \pmod{p};$$

and that is, unless the coefficients of $F(x)$ are all divisible by p. In other words the congruence

$$F(\rho)=r_0+r_1\rho+r_2\rho^2+\cdots+r_{m-1}\rho^{m-1}\equiv 0 \pmod{\mathfrak{p}},$$

where r_i $(i=0, 1, \cdots, m-1)$ are rational integers, is only

[1] Bachmann, *Allgemeine Arith. der Zahlenk.*, p. 241.

possible, if r_i are all divisible by p. And this means that the m powers $1, \rho, \rho^2, \cdots, \rho^{m-1}$ are *independent* (mod. $\mathfrak{p}$) integers. From this it is clear that every integral function $\Phi(\rho)$ with rational integral coefficients is congruent to one and only one expression of the form

$$\Phi(\rho) \equiv a_0 + a_1\rho + \cdots + a_{m-1}\rho^{m-1} \text{ (mod. } \mathfrak{p}),$$

where the a's are reduced (mod. p). Accordingly, p^m is the number of classes into which all functions $\Phi(\rho)$ may be distributed (mod. $\mathfrak{p}$).

ART. **62.** In particular let $P(x)$ be an irreducible function of degree f (mod. p), where f is the degree of the prime ideal $\mathfrak{p}$. Then (Art. 46) the roots of the equation $P(x) = 0$ are primitive numbers that satisfy

$$x^{p^f-1} \equiv 1 \text{ (mod. } \mathfrak{p}).$$

In this case the f integers

$$1, \rho, \rho^2, \cdots \rho^{f-1}$$

are independent, and a congruence of the form

$$F(\rho) = r_0 + r_1\rho + r_2\rho^2 + \cdots + r_{f-1}\rho^{f-1} \equiv 0 \text{ (mod. } \mathfrak{p})$$

cannot exist unless the rational integers r_i are all divisible by p.

Due to the results of Art. 59, there exist f congruences (mod. $\mathfrak{p}$) of the form

$$(1) \qquad \begin{cases} 1 \equiv r_{01}\gamma_1 + r_{02}\gamma_2 + \cdots + r_{0f}\gamma_f, \\ \rho \equiv r_{11}\gamma_1 + r_{12}\gamma_2 + \cdots + r_{1f}\gamma_f, \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \rho^{f-1} \equiv r_{f-1,\,1}\gamma_1 + r_{f-1,\,2}\gamma_2 + \cdots + r_{f-1,\,f}\gamma_f, \end{cases}$$

where the r's are rational integers.

The determinant of these congruences cannot be divisible by p, otherwise (Art. 60) there would exist f

rational integers $r_0, r_1, \cdots, r_{f-1}$ such that

$$r_0+r_1\rho+\cdots+r_{f-1}\rho^{f-1}\equiv 0 \pmod{\mathfrak{p}}.$$

Solving the f congruences (1) for $\gamma_1, \gamma_2, \cdots, \gamma_f$, it is seen (Art. 59) that for every integer γ of $\mathfrak{o}$ there exists a congruence of the form

$$(2) \qquad r\gamma\equiv a+a_1\rho+a_2\rho^2+\cdots a_{f-1}\rho^{f-1} \pmod{\mathfrak{p}}.$$

Since r and p are relatively prime, there exist two integers s and q such that

$$rs+pq=1.$$

This relation combined with (2) shows that every integer γ of $\mathfrak{o}$ has the form

$$(3) \qquad \gamma\equiv g+g_1\rho+g_2\rho^2+\cdots+g_{f-1}\rho^{f-1} \pmod{\mathfrak{p}},$$

where the g's are rational integers, reduced (mod. p).

With this it is proved that *every integer γ of the fixed realm is congruent (mod. $\mathfrak{p}$) to one and only one (Art. 59) expression of the form (3).*

ART. 63. It is possible that the integer $P(\rho)$, which is divisible by $\mathfrak{p}$, might also be divisible by $\mathfrak{p}^2$. It may be proved, however, that the root of the congruence

$$P(x)=a_0+a_1x+a_2x^2+\cdots+x^f\equiv 0 \pmod{\mathfrak{p}}$$

may be so chosen that $P(\rho)$ is divisible by no higher power of $\mathfrak{p}$ than the first. For, if ρ_0 is a root such that $P(\rho)$ is divisible by $\mathfrak{p}^2$, we may put

$$\rho=\rho_0+\tau,$$

where τ is an integer of $\mathfrak{o}$ that is divisible by $\mathfrak{p}$ but *not* by $\mathfrak{p}^2$. Observe that, if ρ_0 is a primitive number, then is ρ also one, since

$$\rho^k\equiv\rho_o^k \pmod{\mathfrak{p}}$$

for every positive integral exponent k. By the Taylor Theorem it is seen that

$$P(\rho)=P(\rho_0+\tau)\equiv P(\rho_0)+\tau P'(\rho_0)+((\tau^2)) \pmod{\mathfrak{p}}.$$

If $P(\rho_0)\equiv 0 \pmod{\mathfrak{p}^2}$, it follows that

$$P(\rho)\equiv \tau P'(\rho_0) \pmod{\mathfrak{p}}.$$

It is clear that $P'(\rho_0)$ is not (Vol. I, Art. 40) divisible by $\mathfrak{p}$, since $P(x)\equiv 0 \pmod{p}$ is an irreducible congruence $\pmod{p}$. With this it is proved that $P(\rho)$ is divisible by $\mathfrak{p}$ but *not* by $\mathfrak{p}^2$.

ART. **64.** It will be proved next that *every integer* γ *of* $\mathfrak{o}$ *is congruent* (*mod.* $\mathfrak{p}^m$) *to an integral function of* ρ *with integral coefficients.*

To prove this, form the expression

$$(1)\qquad \alpha_0+\alpha_1 P(\rho)+\alpha_2 P(\rho)^2+\cdots+\alpha_{m-1}P(\rho)^{m-1},$$

and for the algebraic integers α_i write all values

$$\alpha_i = a_{i0}+a_{i1}\rho+a_{i2}\rho^2+\cdots+a_{i,f-1}\rho^{f-1},$$

in which the rational integer a_{ij} take respectively the values $0, 1, \cdots, p-1$. The expression (1) accordingly takes p^{mf} values, which may be shown as follows to be incongruent $(\text{mod. } \mathfrak{p}^m)$. Were two such expressions

$$(2)\qquad \begin{cases} \alpha_0'+\alpha_1' P(\rho)+\cdots+\alpha_{m-1}' P(\rho)^{m-1}, \\ \alpha_0''+\alpha_1'' P(\rho)+\cdots+\alpha_{m-1}'' P(\rho)^{m-1}, \end{cases}$$

congruent $(\text{mod. } \mathfrak{p}^m)$, they must of necessity be congruent $(\text{mod. } \mathfrak{p})$. Since $P(\rho)$ is divisible by $\mathfrak{p}$, it must follow that $\alpha_0'=\alpha_0''$. Since $P(\rho)$ is divisible by $\mathfrak{p}$ but not by $\mathfrak{p}^2$, there results the congruence

$$\alpha_1'+\alpha_2' P(\rho)+\cdots+\alpha_{m-1}' P(\rho)^{m-2} \equiv \alpha_1''+\alpha_2'' P(\rho)+\cdots+\alpha_{m-1}'' P(\rho)^{m-2} \pmod{\mathfrak{p}^{m-1}}.$$

Through repetition of the above process, it follows that

$$\alpha_1'=\alpha_1'', \qquad \alpha_2'=\alpha_2'', \qquad \cdots, \qquad \alpha_{m-1}'=\alpha_{m-1}'',$$

and with this the identity of the two expressions (2).

Since the number of incongruent $(\text{mod. } \mathfrak{p}^m)$ integers in $\mathfrak{o}$ is $(\mathfrak{p}^m, \mathfrak{o}) = N(\mathfrak{p}^m) = p^{mf}$, it is clear that every integer of the fixed realm is congruent $(\text{mod. } \mathfrak{p}^m)$ to one of the expressions indicated in (1). Due to the fact that ρ must

be an integer such that $P(\rho)$ is divisible by $\mathfrak{p}$ but not by $\mathfrak{p}^2$, it is seen that instead of ρ we may write any other integer $\rho' = \rho + \tau$, where τ is divisible by $\mathfrak{p}^2$. For in this case

$$P(\rho') \equiv P(\rho) \pmod{\mathfrak{p}^2},$$

so that $P(\rho')$ like $P(\rho)$ is divisible by $\mathfrak{p}$ but not by $\mathfrak{p}^2$. (See Hilbert, *Bericht*, p. 193.)

ART. **65.** Observe that if p is the smallest rational integer that is divisible by $\mathfrak{p}$, it is necessarily a prime (Art. 29). Write

$$\mathfrak{o}p = \mathfrak{p}^m \mathfrak{q},$$

where $\mathfrak{q}$ is *not* divisible by $\mathfrak{p}$. It is seen that there exists an integer of $\mathfrak{q}$, say γ, which is *not* divisible by $\mathfrak{p}$ and accordingly also *not* by $\mathfrak{p}^2$. Due to the Fermat Theorem, it follows that

$$\gamma^{p^f(p^f-1)} \equiv 1 \pmod{\mathfrak{p}^2}.$$

Multiply this congruence by ρ' and put $\rho = \rho' \gamma^{p^f(p^f-1)}$. We thus derive

$$\rho \equiv \rho' \pmod{\mathfrak{p}^2},$$

where ρ' has the same significance as in the preceding article. Observe that the constant term in $P(x)$ is not divisible by p and therefore it is not divisible by any ideal factor of p, such as $\mathfrak{q}$. On the other hand, since ρ is divisible by γ and therefore also by $\mathfrak{q}$, it follows that $P(\rho)$ is not divisible by $\mathfrak{q}$. Since $P(\rho)$ is divisible by $\mathfrak{p}$ but *not* by $\mathfrak{p}^2$, it is seen that $\mathfrak{p}$ is the greatest common divisor of $\mathfrak{o}p$ and $\mathfrak{o}P(\rho)$.

Accordingly, we have the theorem: *If $\mathfrak{p}$ is a prime ideal of the fth degree and if $P(x)$ is an arbitrary prime function (mod. p) of the fth degree, there is a root ρ of $P(x)$ such that every integer of the fixed realm is congruent (mod. $\mathfrak{p}^m$), m an arbitrary positive rational integer, to an integral rational function of ρ with rational integral coefficients, while at the*

same time $\mathfrak{p}$ *is the greatest common divisor of the two principal ideals* $\mathfrak{o}p$ *and* $\mathfrak{o}P(\rho)$, *and that is*

$$\mathfrak{p} = (p, P(\rho)).$$

Due to this theorem it is seen that any prime ideal may be expressed as the greatest common ideal divisor of two principal ideals. If further we regard $\mathfrak{p}^2$ as the greatest common divisor of $\mathfrak{o}p^2$ and $\mathfrak{o}P(\rho)^2$, it follows without difficulty that any ideal $\mathfrak{i}(=\mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\cdots\mathfrak{p}_r^{a_r})$ may be expressed as the greatest common divisor of two principal ideals, where one is a rational integer. (See Bachmann, *Allgemeine Arithmetik der Zahlenkörper*, p. 246.)

ART. **66.** It may be well to close this chapter with a statement made by Dedekind, "Ueber der Begründung der Idealtheorie," *Nachr. von der Königl. Gesellschaft der Wiss. zu Göttingen*, 1895, p. 106, to the effect that the greatest difficulty in establishing the theory was overcome in the proof of the theorems:

I. If the ideal $\mathfrak{c}$ is divisible by the ideal $\mathfrak{a}$, there exists an ideal $\mathfrak{b}$ such that $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$.

Dedekind declares that for years he had returned to this cardinal point with the intention of getting a proof simply and directly from the concept of the whole number (integer). (See Art. 13.)

II. Every ideal $\mathfrak{m}$ may by multiplication with an ideal $\mathfrak{n}$ be changed into a principal ideal. (See Arts. 14 ff.)

III. Every finite modul $\mathfrak{m}$ which is different from zero, may by multiplication by a modul $\mathfrak{n}$, whose elements are formed from those of $\mathfrak{m}$ in a rational manner, be changed into a modul $\mathfrak{m}\mathfrak{n}$ which contains $[1]$ and consists of only algebraic integers. (See Art. 14.)

IV. From any m algebraic numbers $\mu_1, \mu_2, \cdots, \mu_m$, which do not all vanish, it is possible to form in a rational manner m other algebraic numbers $\nu_1, \nu_2, \cdots, \nu_m$, such

that

$$\mu_1\nu_1+\mu_2\nu_2+\cdots+\mu_m\nu_m=1,$$

and at the same time the m^2 products $\mu_i\nu_j$ $(i, j=1, 2, \cdots, n)$ are integers. (Vol. I, Art. 163.)

Observe that any one of these theorems can be derived from the other three. By making use of the modul concept we have seen (Art. 14) how simply Theorems III and IV may be derived in comparison with Theorems I and II, in which the ideal concept is employed. However, as simple as Theorem III is for the case $m=2$, Dedekind says that for a long time he was unable to extend it to the case where the modul consists of three or more elements and that it was only step by step by doing away with limiting assumptions that he was able eventually to come to a proof of the above theorems in all their generality.[1]

To these four theorems may be added

THEOREM V. *If the product GH of two integral rational functions of an arbitrary number of independent variables have as coefficients only algebraic integers, then is every product consisting of a coefficient of G by one of H an algebraic integer.*

This theorem used to advantage in the proof of Theorem I greatly simplifies Kronecker's Theory (*Grundzüge*, §§ 14 et seq., and §§ 20 et seq.). See also the remarks of Hurwitz, p. 230 of the *Göttingen Nachrichten*, 1895.

EXAMPLES

1. If $\mathfrak{a}$ and $\mathfrak{b}$ are arbitrary ideals, there exists an integer ω in $\mathfrak{o}$, such that the greatest common divisor

$$\mathfrak{a}\mathfrak{b}+\omega\mathfrak{o}=\mathfrak{a}.$$

[1] See also Landau, "Nachruf auf Dedekind," *Gött. Nachr.*, 1917. Noether, *Math. Ann.*, Vol. 96, p. 26, builds an ideal theory from *five* axioms. On p. 28 he speaks of the "etwas mehr aussagende Modulsätze."

To prove this, write

$$\mathfrak{ab}=\mathfrak{p}_1^{g_1}\mathfrak{p}_2^{g_2}\cdots\mathfrak{p}_k^{g_k}, \qquad \mathfrak{a}=\mathfrak{p}_1^{d_1}\mathfrak{p}_2^{d_2}\cdots\mathfrak{p}_k^{d_k},$$

where the $\mathfrak{p}$'s are prime ideals and $d_i(\leqq g_i)$ are rational integers or zero ($i=1, 2, \cdots, k$). For each of the integers i choose a number γ_i which is found in $\mathfrak{p}_i^{d_i}$ but not in $\mathfrak{p}_i^{d_i+1}$. Observe that there are more integers in $\mathfrak{p}_i^{d_i}$ than in $\mathfrak{p}_i^{d_i+1}$. This may be omitted for the cases $d_i=0$. There exists an integer ω (Art. 33) such that $\omega\equiv\gamma_1 \pmod{\mathfrak{p}_1^{d_1+1}}$, $\omega\equiv\gamma_2 \pmod{\mathfrak{p}_2^{d_2+1}}$, $\cdots$, $\omega\equiv\gamma_k \pmod{\mathfrak{p}_k^{d_k+1}}$. Then observe that $\omega\mathfrak{o}$ is such that $\mathfrak{ab}+\omega\mathfrak{o}=\mathfrak{a}$. A consequence of this is the theorem: If $\mathfrak{a}$ and $\mathfrak{b}$ are arbitrary ideals, another ideal $\mathfrak{i}$ may be found such that $\mathfrak{ai}$ is a principal ideal $\omega\mathfrak{o}$ and $\mathfrak{b}+\mathfrak{i}=\mathfrak{o}$. For from above $\mathfrak{a}(\mathfrak{b}+\mathfrak{i})=\mathfrak{ab}+\omega\mathfrak{o}=\mathfrak{a}$, so that $\mathfrak{b}+\mathfrak{i}=\mathfrak{o}$. Prove that from the latter theorem the former result may also be derived.

2. As a consequence of Example 1, prove that the least common multiple

$$\mathfrak{ab}-\omega\mathfrak{o}=\mathfrak{b}\omega.$$

3. Using Examples 1 and 2 prove that

$$(\mathfrak{o}, \mathfrak{ab})=(\mathfrak{o}, \mathfrak{a})(\mathfrak{o}, \mathfrak{b}),$$

and that is,

$$N(\mathfrak{ab})=N(\mathfrak{a})N(\mathfrak{b}).$$

4. A direct proof of the theorem as stated in Example 3 and in Art. 22 is very desirable.

5. Using Example 1 prove that every ideal may be expressed as the greatest common divisor of two principal ideals.

The reader may consult with advantage Lasker, "Zur Theorie der Moduln und Ideale," *Math. Ann.*, Vol. 60, p. 20; and he may also prove anew the fourteen fundamental theorems given in Dedekind's *Werke*, Vol. I, pp. 115 ff.

CHAPTER IV

THE KRONECKER THEORY OF FORMS

ART. **67. Definitions.** By a methodical use of indeterminate coefficients, Kronecker [1] wished to put the divisors of algebraic integers in a simple and natural form and in such a way that the intrinsic and abstract properties of the generalized Kummer numbers, of the Dedekind ideals, etc., like those of the rational numbers, take concrete arithmetic expression. This principle lies simply in the fact that the realm of the algebraic quantities may be sufficiently extended that the laws of division, which exist for rational integers and for rational integral functions, may be so modified as to work effectively in the transition to the algebraic integers.

An integral function $F(u, u_1, u_2, \cdots, u_r)$ of the indeterminates $u, u_1, u_2, \cdots, u_r$, whose coefficients $\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_r$ are algebraic integers of a fixed realm, was called by Kronecker "*a form of the realm.*" The indeterminates $u, u_1, u_2, \cdots, u_r$ play a comparatively unimportant rôle in this discussion, as attention is directed in the main to the coefficients, the algebraic integers.

If the algebraic integers of the form F be replaced by their conjugates, there results the so-called *conjugate* forms $F^{(1)}, F^{(2)}, \cdots, F^{(n-1)}$, where n is the degree of the stock-realm.

[1] Kronecker, *Grundzüge einer arithmetischer Theorie der algebraischen Grössen*, Part II, § 14 and following. *Crelle's Journal*, Vol. 92; *Werke*, Vol. II, p. 237. See also the expository memoir by Molk, "Sur une notion qui comprend celle de la divisibilité, etc.," *Acta Math.*, Vol. 6.

It is clear that

$$F \cdot F^{(1)} \ldots F^{(n-1)} = gU,$$

where U is an integral function of $u_1, u_2, \cdots$, with rational integral coefficients, and where the rational integer g has been so chosen that the greatest common divisor of the coefficients of U is 1. Kronecker (*Grundzüge*, p. 46) called g the *norm* of the form F. When $g=1$, the form F is called a *unit* form.

Two forms are said to be *equivalent in a restricted sense*, which equivalence is denoted by the symbol $\simeq$, when their quotient is equal to the quotient of two unit forms. In particular, every unit form is $\simeq 1$; and that is, an integral algebraic quantity (form) whose norm = 1, is an algebraic unit (Kronecker, p. 48).

A form H is said to be divisible by a form F, if there exists a form G such that $H \simeq FG$.

A form P is called a *prime form* if P in the restricted sense of equivalence, is divisible by no form save itself and unity. Hence, a form is either divisible by P or it has no factor in common with P save unity.

ART. **68. The Content of a Form.** The relation between the Kronecker theory of forms and the theory of ideals is put in evidence, if we note that to each form of the realm there corresponds a definite ideal

$$\mathfrak{a} = (\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_r);$$

and to every ideal there corresponds an indefinite number of forms. Such forms are, for example,

$$F(u, u_1, u_2, \cdots, u_r) = \alpha_1 V_1 + \alpha_2 V_2 + \cdots + \alpha_r V_r,$$

where V_i consists of any product of any powers of $u, u_1, u_2, \cdots$, and

$$V_i \neq V_j \qquad (i, j = 1, 2, \cdots, r).$$

The ideal $\mathfrak{a}$ was called by Hilbert [1] the *content* of the form.

[1] Hilbert, "Die Theorie der algebraischen Zahlkörper," *Jahresb. der deutsch. Mathematiker-Vereinigung*, Vol. 4, p. 187.

THEOREM I. *The content of the product of forms is equal to the product of the contents of the forms.*

If the theorem is proved for two forms the general proof follows.

Let $F_1(u, u_1, u_2, \cdots)$, $F_2(u, u_1, u_2, \cdots)$ be two forms with contents

$$\mathfrak{a}' = (\alpha_1', \alpha_2', \cdots, \alpha_r'), \qquad \mathfrak{a}'' = (\alpha_1'', \alpha_2'', \cdots, \alpha_s'');$$

and let the content of the product

$$F(u_1, u_2, \cdots) = F_1(u_1, u_2, \cdots)F_2(u_1, u_2, \cdots)$$

be

$$\mathfrak{a} = (\alpha_1, \alpha_2, \cdots, \alpha_t).$$

Write $u = x$, $u_1 = x^k$, $u_2 = x^{k^2}$, $\cdots$, and choose k so large that the number of terms in $F_1(x)$, $F_2(x)$, and $F(x)$ are the same as those in $F_1(u_1, u_2, \cdots)$, $F_2(u_1, u_2, \cdots)$, $F(u_1, u_2, \cdots)$, respectively. Accordingly we may write

$$F(x) = \beta_1 x^{h_1} + \beta_2 x^{h_2} + \cdots + \beta_t x^{h_t},$$

where the β's are, neglecting the order, the same as the α's of $F(u_1, u_2, \cdots)$. Similarly, it is seen that

$$F_1(x) = \beta_1' x^{h_1'} + \beta_2' x^{h_2'} + \cdots + \beta_r' x^{h_r'},$$
$$F_2(x) = \beta_1'' x^{h_1''} + \beta_2'' x^{h_2''} + \cdots + \beta_s'' x^{h_s''},$$

the β''s being the same as the α''s and the β'''s being the same as the α'''s.

Let $\mathfrak{p}$ be any prime ideal of the realm and let the ideal $\mathfrak{a}$ be divisible by $\mathfrak{p}^a$ while $\mathfrak{a}'$ is divisible by $\mathfrak{p}^{a'}$ and the ideal $\mathfrak{a}''$ by $\mathfrak{p}^{a''}$, these being the highest powers of $\mathfrak{p}$ that are found in the respective ideals. The exponents a, a', and a'' are of course zero, when $\mathfrak{p}$ does not divide these ideals. It follows that all the elements β_i' are divisible by $\mathfrak{p}^{a'}$ but at least one of them is *not* divisible by $\mathfrak{p}^{a'+1}$; otherwise the ideal $\mathfrak{a}'$ would be divisible by $\mathfrak{p}^{a'+1}$. Similarly, all the elements β_i'' are divisible by $\mathfrak{p}^{a''}$ but at least one is not divisible by $\mathfrak{p}^{a''+1}$.

Let β_k' be the first of the elements β' that is not divisible by $\mathfrak{p}^{a'+1}$ and let β_l'' be the first of the elements β'' which is not divisible by $\mathfrak{p}^{a''+1}$, then, and in a similar manner as in the proof of the Gaussian Formula of Vol. I, Art. 4, it is seen that the term $\beta_i x^{h_i}$ of the function $F(x)$, whose exponent $h_i = h_k' + h_l''$, must have as coefficient β_i an algebraic integer, that is divisible by $\mathfrak{p}^{a'+a''}$ but by no higher power of $\mathfrak{p}$. And further, observe that all the coefficients of $F(x)$ are divisible by $\mathfrak{p}^{a'+a''}$.

It follows that the ideal

$$(\beta_1, \beta_2, \cdots, \beta_t) = \mathfrak{a}$$

is divisible by $\mathfrak{p}^{a'+a''}$ but by no higher power of $\mathfrak{p}$. It is thus seen [1] that every prime ideal $\mathfrak{p}$ occurs to the same power as a factor of $\mathfrak{a}$, as it appears in the factorization of $\mathfrak{a}'$ and $\mathfrak{a}''$ taken together. With this it follows that $\mathfrak{a} = \mathfrak{a}'\mathfrak{a}''$.

Due to the Primary Theorem in ideals, namely, that *associated with every ideal* $\mathfrak{i}$ *there is another ideal* $\mathfrak{i}_1$, *such that* $\mathfrak{i}\mathfrak{i}_1$ *is a principal ideal*, follow, in connection with Theorem I above, the theorems:

THEOREM II. *If F is a given form, another form F_1 may be so determined that the product of the two forms is equivalent in a restricted sense to an integer.*

THEOREM III. *If the product of two forms is divisible by a prime form P, at least one of the forms is divisible by P.*

THEOREM IV. *In the sense of restricted equivalence, every form may be factored in one and only one way into a product of prime forms.*

ART. 69. The definition of a unit form of the preceding article in the ideal terminology may be thus stated: *A unit form is one whose content is* $\mathfrak{o}$. This includes forms with rational integral coefficients whose greatest common divisor is unity, the primitive forms of Vol. I, Art. 5.

[1] See also Bachmann, *Allgemeine Theorie der Zahlenkörper*, p. 252.

Let $f(x)=0$ be the irreducible equation of the nth degree whose root α determines the fixed realm of rationality $\Re(\alpha)$.

THEOREM. *If* $F(u, u_1, u_2, \cdots)$ *is a unit form, its norm is a primitive form and inversely.*

Proof. Write

$$\Phi(u, u_1, u_2, \cdots) = F^{(1)}(u, u_1, u_2, \cdots)F^{(2)}(u, u_1, \cdots)\cdots F^{(n-1)}(u, u_1, \cdots),$$

so that

$$N\{F(u, u_1, \cdots)\} = F(u, u_1, \cdots)\Phi(u, u_1, \cdots).$$

Observe that the coefficients $\beta_1, \beta_2, \cdots, \beta_s$ say, of $\Phi(u, u_1, \cdots)$ are algebraic integers of $\Re(\alpha)$, so that the content of this function is the ideal $(\beta_1, \beta_2, \cdots\beta_s)$ of the fixed realm. From the preceding article it is seen that

$$(\alpha_1, \alpha_2, \cdots, \alpha_r)(\beta_1, \beta_2, \cdots, \beta_s) = \mathfrak{o}m,$$

where m is an integer. If $m=1$, and that is, if $N\{F(u, u_1, u_2, \cdots)\}$ is a primitive form, it follows that

$$\mathfrak{a} = (\alpha_1, \alpha_2, \cdots, \alpha_r) = \mathfrak{o}.$$

Reciprocally, if $\mathfrak{a}=\mathfrak{o}$, it follows that $(\beta_1, \beta_2, \cdots, \beta_s) = m\mathfrak{o}$; and consequently, each of the integers β_i is divisible by m, the same being true of the conjugate values $\beta_i^{(1)}, \beta_i^{(2)}, \cdots\beta_i^{(n)}$. It follows also that the product of the conjugate values

$$\Phi^{(1)}\Phi^{(2)}\ldots\Phi^{(n-1)} = \frac{N\{F(u, u_1, \cdots)^{n-1}\}}{F^{(1)}F^{(2)}\ldots F^{(n-1)}} = m^{n-2}F(u, u_1, \cdots)U^{n-2},$$

where U is a unit (primitive) form. Observe that the left-hand side of this equation is divisible by m^{n-1}, while the right hand side contains only m^{n-2} as a factor. Hence, it is seen that $m=1$ and consequently $N\{F(u, u_1, u_2, \cdots)\}$ is a primitive form.

From this it is clear that *two forms of equal content, differ only by factors which are unit forms, and inversely, two forms which differ thus from each other have the same content.* For, if there exists the equation

$$F_1 U = F U_1, \tag{1}$$

where U and U_1 are unit forms, it follows from Theorem I of Art. 68 that the content of both sides of this equation is the same and accordingly F and F_1 have the same content.

Inversely, if F and F_1 have the same content, the equation just written must exist. For, since $F\Phi$ and $F_1\Phi$ have the same content, and since

$$F\Phi = mU,$$

it follows that

$$F_1\Phi = mU_1 = \frac{F\Phi U_1}{U}, \qquad \text{or} \qquad F_1 U = F U_1.$$

This coincides with the definition of two equivalent forms; namely, *two forms are equivalent, if their quotient is equal to the quotient of two unit forms.*

It also shows that equivalent forms have the same norm, since the norm of a unit form is 1.

ART. **70.** THEOREM. *The norm of a form is the norm of its content, and that is, of the ideal whose elements are the coefficients of the form.*

Let $\mathfrak{a} = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ be the content of the form, which may be written

$$F = u_1\alpha_1 + u_2\alpha_2 + \cdots + u_n\alpha_n.$$

Let $\omega_1, \omega_2, \cdots \omega_n$ be the basis of all integers of the fixed realm; and observe that $\alpha_i\omega_j$ $(i, j = 1, 2, \cdots, n)$ are integers of $\mathfrak{a}$. We may accordingly write

$$\omega_i F = U_{1i}\alpha_1 + U_{2i}\alpha_2 + \cdots + U_{ni}\alpha_n \quad (i = 1, 2, \cdots, n),$$

where the U's are linear functions of $u_1, u_2, \cdots, u_n$, with

rational integral coefficients. The determinant

$$U = |U_{ik}| \qquad (i, k = 1, 2, \cdots, n)$$

is a unit-form of the nth degree in the u's. For, suppose that this is not the case, and let d be the divisor (Vol. I, Art. 5) of this determinant.

If p is a prime rational integer that is a divisor of d, we may determine (Vol. I, Art. 56) forms $f_1, f_2, \cdots, f_n$, which are not all divisible by p, such that

$$U_{i1}f_1 + U_{i2}f_2 + \cdots + U_{in}f_n \equiv 0 \pmod{p} \quad (i = 1, 2, \cdots, n).$$

It follows that

$$F(f_1\omega_1 + f_2\omega_2 + \cdots + f_n\omega_n)$$
$$= \sum_{i=1}^{i=n} (U_{i1}f_1 + U_{i2}f_2 + \cdots + U_{in}f_n)\alpha_i \equiv 0 \pmod{p\mathfrak{a}}.$$

Observing that the content of F is $\mathfrak{a}$, it is seen from the expression just written that

$$f_1\omega_1 + f_2\omega_2 + \cdots + f_n\omega_n \equiv 0 \pmod{p}.$$

From this it would follow that each of the forms $f_1, f_2, \cdots, f_n$ is divisible by p, which is contrary to the hypothesis.

We may next form the determinant

$$\begin{vmatrix} \omega_1 F, & \omega_2 F, & \cdots, & \omega_n F \\ \omega_1' F', & \omega_2' F', & \cdots, & \omega_n' F' \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \omega_1^{(n-1)} F^{(n-1)}, & \omega_2^{(n-1)} F^{(n-1)}, & \cdots, & \omega_n^{(n-1)} F^{(n-1)} \end{vmatrix}$$

$$= \begin{vmatrix} U_{11}, & U_{12}, & \cdots, & U_{1n} \\ U_{21}, & U_{22}, & \cdots, & U_{2n} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ U_{n1}, & U_{n2}, & \cdots, & U_{nn} \end{vmatrix} \begin{vmatrix} \alpha_1, & \alpha_2, & \cdots, & \alpha_n \\ \alpha_1', & \alpha_2', & \cdots, & \alpha_n' \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \alpha_1^{(n-1)}, & \alpha_2^{(n-1)}, & \cdots, & \alpha_n^{(n-1)} \end{vmatrix}.$$

Further, since

$$\alpha_i = c_{1i}\omega_1 + c_{2i}\omega_2 + \cdots + c_{ni}\omega_n \quad (i = 1, 2, \cdots, n),$$

where the c's are rational integers, the above determinantal equation takes the form

$$F \cdot F^{(1)} \ldots F^{(n-1)} = U \, |c_{ik}| \, ;$$

and, as (Vol. I, Art. 152)

$$N(\mathfrak{a}) = (\mathfrak{o}, \mathfrak{a}) = |c_{ik}| ,$$

it is seen that

$$N\{F\} \leqq N(\mathfrak{a}).$$

In this we have a new definition of the norm of an ideal in that it is the generalization of the norm of an integer extended to that of the norm of an integral form; and instead of considering an ideal as the complex of the infinite number of algebraic integers that constitute it, we may take the closed algebraic expression, the form, whose content is this ideal.

ART. **71.** It is evident that all the algebraic integers of the fixed realm, and that is of $\mathfrak{o} = (\omega_1, \omega_2, \cdots, \omega_n)$, are had, if in the linear form

$$\xi = \omega_1 u_1 + \omega_2 u_2 + \cdots + \omega_n u_n, \tag{1}$$

all possible rational integral values are given to the indeterminates u_i $(i = 1, 2, \cdots, n)$. The form ξ was called by Kronecker (*Grundzüge*, p. 109) the *fundamental form* of the fixed realm.

Denote the conjugate forms by

$$\begin{aligned} \xi^{(1)} &= \omega_1^{(1)} u_1 + \omega_2^{(1)} u_2 + \cdots + \omega_n^{(1)} u_n, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \xi^{(n-1)} &= \omega_1^{(n-1)} u_1 + \omega_2^{(n-1)} u_2 + \cdots + \omega_n^{(n-1)} u_n ; \end{aligned}$$

and write the equation

$$\begin{aligned} F(x) &= (x - \xi)(x - \xi^{(1)}) \cdots (x - \xi^{(n-1)}) \\ &= x^n + U_1 x^{n-1} + U_2 x^{n-2} + \cdots + U_n = 0, \end{aligned}$$

where $U_1, U_2, \cdots, U_n$ are integral functions of $u_1, u_2, \cdots, u_n$, with rational integral coefficients.

This is Kronecker's *fundamental equation* of the realm. It is satisfied by the fundamental form. When all

integral rational values are given to the indeterminates u_i, the quantity ξ goes over all the algebraic integers of the fixed realm, and accordingly the fundamental equation represents in turn the algebraic equations of the nth degree which these algebraic numbers satisfy. Instead of investigating all such equations to determine, for example, whether in respect to a prime integer p, as modulus, the corresponding algebraic integer satisfied a congruence which admitted prime factors (modulo p), it was Kronecker's thought to make this investigation for the congruence

$$F(x) \equiv 0 \pmod{p},$$

and therefrom draw conclusions for the special cases.

The building of the fundamental equation with Kronecker forms the original aim of an investigation, which in its extent shows the correct starting point, the true general form of the complex numbers and at the same time, through the association of linear forms and divisors, it leads to the method of reaching "completely" and "in the simplest manner," the scope (*Ziele*) of the theory. To this end the present work is directed.

LEMMA I. *If* $\mathfrak{p}$ *is a prime ideal of the* f*th degree, that is, if* $\mathfrak{p}$ *is a divisor of the rational prime integer* p *and* $N(\mathfrak{p}) = p^f$, *there exists with respect to* p, *a prime function* $\Pi(x; u_1, u_2, \cdots, u_n)$ *of the* f*th degree in* x, *which, if for* x *is substituted the fundamental form* $\xi = \omega_1 u_1 + \omega_2 u_2 + \cdots + \omega_n u_n$, *has the following properties: The coefficients of the product of the powers of* $u_1, u_2, \cdots, u_n$ *are each divisible by* $\mathfrak{p}$ *but not by* $\mathfrak{p}^2$, *and also they are not divisible by any other prime ideal factor of* p.

Proof. Let $p = \mathfrak{p}^e \mathfrak{q}$, where $\mathfrak{q}$ is not divisible by $\mathfrak{p}$. Further, let ρ be a primitive number with respect to $\mathfrak{p}$ as defined in Art. 62, $P(\rho) \equiv 0 \pmod{\mathfrak{p}}$ being the function

$P(x)=(x-\rho)(x-\rho^p)\ \cdots\ (x-\rho^{p^{f-1}})$ (mod. $\mathfrak{p}$), the prime function defined in Arts. 42, 43.

Since every integer in $\mathfrak{o}$ is congruent (mod. $\mathfrak{p}$) to an integral function in ρ (Art. 62), we may put

$$\xi=\omega_1u_1+\omega_2u_2+\cdots+\omega_nu_n\equiv G(\rho;u_1,u_2,\cdots,u_n)\ (\text{mod. }\mathfrak{p}),$$

where G is an integral function in $\rho, u_1, \cdots, u_n$. Form the expression $(x-G(\rho;\ u_1,\ \cdots,\ u_n))(x-G(\rho^p;\ u_1,\ \cdots,\ u_n))\cdots(x-G(\rho^{p^{f-1}};\ u_1,\ \cdots,\ u_n))$, which (mod. $\mathfrak{p}$) is congruent to an integral function in $x,\ u_1,\ \cdots,\ u_n$. Denote this function by $\Pi(x;\ u_1,\ \cdots,\ u_n)$; and observe that, when for x is written the fundamental form ξ, we have

$$\Pi(\xi;\ u_1,\ u_2,\ \cdots,\ u_n)\equiv 0\ (\text{mod. }\mathfrak{p}).$$

Write

$$\rho=a_1\omega_1+a_2\omega_2+\cdots+a_n\omega_n;$$

and observe that

$$\xi=u_1\omega_1+u_2\omega_2+\cdots+u_n\omega_n$$

becomes $\xi=\rho$, where $u_i=a_i$ $(i=1,\ 2,\ \cdots,\ n)$. It follows since ρ is a root of $P(x)=0$, that

$$\Pi(x;\ a_1,\ a_2,\ \cdots,\ a_n)\equiv P(x)\ (\text{mod. }\mathfrak{p}),$$

and Art. 65 that

$$\mathfrak{p}=(p,\ \Pi(\rho;\ a_1,\ a_2,\ \cdots,\ a_n)).$$

It further follows from this last expression that the coefficients of the powers and product of $u_1, u_2, \cdots, u_n$ in $\Pi(\xi;\ u_1,\ u_2,\ \cdots,\ u_n)$ are *not* all divisible by $\mathfrak{p}^2$ neither can they be divisible by any other prime ideal factor of p save $\mathfrak{p}$. And $P(x)$ being a prime function (mod. p), the same must likewise be true of $\Pi(x;u_1,\ \cdots,u_n)$.

ART. **72.** The above Lemma is implicitly stated and proved as follows:

Determine the congruence (mod. $\mathfrak{p}$*) of lowest degree which the fundamental form* ξ *satisfies.*

With Hensel (*Crelle's Journal*, Vol. 113, pp. 64 et seq.) let

$$\varphi(x; u_1, \cdots, u_n) \equiv 0 \pmod{\mathfrak{p}} \tag{1}$$

be an arbitrary congruence of the form

$$\varphi(x; u_1, \cdots, u_n) = U_0 x^m + U_1 x^{m-1} + \cdots + U_m,$$

where the U's are integral functions of the u's with rational integral coefficients; and suppose that this congruence is satisfied (mod. $\mathfrak{p}$), when for x is written ξ; and that is, $\mathfrak{p}$ is the content of the form

$$\varphi(\xi; u_1, u_2, \cdots, u_n).$$

By raising the congruence (1) to the pth power and making use of the Fermat Theorem as in Art. 30, it is seen that

$$\xi_1 = \omega_1^p u_1 + \omega_2^p u_2 + \cdots + \omega_n^p u_n,$$

and in general

$$\xi_k = \omega_1^{p^k} u_1 + \omega_2^{p^k} u_2 + \cdots + \omega_n^{p^k} u_n$$

are the roots of the same congruence. This is the *definition* of the functions $\xi_1, \xi_2, \cdots$.

From this it may be proved that $\xi, \xi_1, \cdots, \xi_{f-1}$ are the roots of the irreducible congruence

$$\Pi(\xi) = (x-\xi)(x-\xi_1)\cdots(x-\xi_{f-1}) \equiv x^f + c_1 x^{f-1} + \cdots + c_f \pmod{\mathfrak{p}}$$

(see Art. 42), where the c's are rational integers reduced, mod. p. (See also Art. 60.)

In this proof observe that every integer, say γ, in $\mathfrak{o}$ satisfies the congruence

$$\gamma^{p^f} \equiv \gamma \pmod{\mathfrak{p}},$$

where f is the degree of the prime ideal $\mathfrak{p}$.

Also observe that the f functions $\xi_0, \xi_1, \cdots, \xi_{f-1}$ are incongruent (mod. $\mathfrak{p}$). For, were $\xi_{\sigma+k} \equiv \xi_\sigma \pmod{\mathfrak{p}}$, it would follow that

$$\omega_i^{p^{\sigma+k}} \equiv \omega_i^{p^\sigma} \pmod{\mathfrak{p}} \qquad (i=1, 2, \cdots, n).$$

If this congruence is raised to the p^{f-g} power, it follows that

$$\omega_i^{p^{f+k}} \equiv \omega_i^{p^f} \text{ (mod. } \mathfrak{p}) \quad \text{or} \quad \omega_i^{p^k} \equiv \omega_i \text{ (mod. } \mathfrak{p}) \quad (i = 1, 2, \cdots, n).$$

And, were this true of the basal elements, it would be true of all integers in $\mathfrak{o}$, which is true only if $k = f$.

It is thus seen that $\mathfrak{p}$ is the content of the form

$$pz + \Pi(\xi),$$

or, as expressed by Kronecker (*Grundzüge*, p. 114),

$$\mathfrak{p} \sim pz + \Pi(\xi)$$

(Hensel, *op. cit.*, p. 72).

LEMMA II. *Every integral function* $\Phi(x; u_1, \cdots, u_n)$ *with integral coefficients, which identically in* $u_1, u_2, \cdots, u_n$ *is congruent to zero, modulo* $\mathfrak{p}$, *when the fundamental form* ξ *is written for* x, *is, with respect to* p, *divisible by* $\Pi(x; u_1, \cdots, u_n)$.

Proof. If this were not true, then Φ and Π would be relatively prime and there would be two integral functions of $u_1, \cdots, u_n$ with rational integral coefficients A and B, such that

$$A\Phi + B\Pi \equiv U(u_1, \cdots, u_n) \text{ (mod. } p).$$

Since both Φ and Π are congruent to zero (mod. $\mathfrak{p}$) when ξ is written for x, it would follow also that $U(u_1, \cdots, u_n) \equiv 0$ (mod. p), which is *not* true.

LEMMA III. *If* Φ *is an integral function in* $x, u_1, u_2, \cdots, u_n$ *with rational integral coefficients, which is identically congruent to zero with respect to* $\mathfrak{p}^e$, *when* ξ *is written for* x, *then with respect to* p, *the function* Φ *is divisible by* Π^e.

Proof. Write

$$\Phi = \Pi^g \Psi,$$

where $g < e$, and Ψ is an integral function in $x, u_1, \cdots, u_n$, which is *not* divisible by Π, modulo p. It follows that all the coefficients of the powers and products of $u_1, \cdots,$

u_n in the expression

$$\{\Pi(\xi; u_1, \cdots, u_n)\}^\sigma \Psi(\xi; u_1, \cdots, u_n)$$

must be divisible by $\mathfrak{p}^e$. This is evidently not true unless each term in the expansion of $\Psi(\xi; u_1, \cdots, u_n)$ is divisible by $\mathfrak{p}$ to at least the first power. And, if this were true, it would follow from Lemma II that Ψ is divisible by Π contrary to the hypothesis.

ART. **73.** It is of interest to prove directly that the form $\Pi(\xi; u_1, \cdots, u_n)$ is divisible by the first and no higher power of $\mathfrak{p}$, and is divisible by no other prime ideal factor of p.

With Hensel (*loc. cit.*) let

$$\tilde{\omega} = a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n,$$

where the a's are rational integers, be an integer which is divisible by the first but no higher power of $\mathfrak{p}$. Consider the congruence that is satisfied (mod. $\mathfrak{p}$) by

$$\xi + \tilde{\omega} = (u_1 + a_1)\omega_1 + (u_2 + a_2)\omega_2 + \cdots + (u_n + a_n)\omega_n,$$

and that is, the congruence

$$\Pi(\xi + \tilde{\omega}; u_1 + a_1, u_2 + a_2, \cdots, u_n + a_n) \equiv 0 \pmod{\mathfrak{p}}.$$

Writing

$$\tilde{\omega}_k = \omega_1^{p^k} a_1 + \omega_2^{p^k} a_2 + \cdots + \omega_n^{p^k} a_n \qquad (k = 1, 2, \cdots),$$

it is seen that $\xi + \tilde{\omega}$, $\xi_1 + \tilde{\omega}_1$, $\cdots$, $\xi_{f-1} + \tilde{\omega}_{f-1}$ are congruent (mod. $\mathfrak{p}$) respectively to $\xi, \xi_1, \cdots, \xi_{f-1}$. The same is true of the symmetric functions of these sets of quantities with the result that (mod. p) the coefficients of

$$\Pi(x; u_1 + a_1, \cdots, u_n + a_n) \quad \text{and} \quad \Pi(x; u_1, \cdots, u_n)$$

are equal; and that is, $\xi + \tilde{\omega}$ satisfies the congruence

$$\Pi(x; u_1, \cdots, u_n) \equiv 0 \pmod{p}.$$

If $\Pi(\xi) \equiv 0 \pmod{\mathfrak{p}^2}$, then also is $\Pi(\xi + \tilde{\omega}) \equiv 0 \pmod{\mathfrak{p}^2}$. Writing

$$\Pi(\xi + \tilde{\omega}) = \Pi(\xi) + \tilde{\omega}\Pi'(\xi) + (\tilde{\omega}^2) \pmod{\mathfrak{p}},$$

it would follow that

$$\Pi'(\xi)=(\xi-\xi_1)(\xi-\xi_2)\cdots(\xi-\xi_{f-1})\equiv 0 \pmod{\mathfrak{p}},$$

which, as shown above, is *not* true, $\Pi(x)$ being irreducible, mod. p.

It may also be proved that $\Pi(\xi;\ u_1,\ \cdots,\ u_n)$ is *not* divisible by $\mathfrak{p}'$, where $\mathfrak{p}'$ is an ideal divisor of p which is different from $\mathfrak{p}$ as follows:

Observe that the fundamental form runs over all the integers of $\mathfrak{o}$, when rational integral values are given to $u_1, u_2, \cdots, u_n$. Accordingly, select an integer $\tilde{\omega}$ which is divisible by $\mathfrak{p}$ but *not* by $\mathfrak{p}'$. Writing $\xi=\tilde{\omega}$, it is seen that $\xi_1, \cdots, \xi_{f-1}$ are all divisible by $\mathfrak{p}$; and in this case

$$\Pi(x)\equiv(x-\xi)(x-\xi_1)\cdots(x-\xi_{f-1})\equiv x^f \pmod{p}.$$

And, were $\Pi(\tilde{\omega})$ divisible by $\mathfrak{p}'$, it would follow that $\tilde{\omega}^f\equiv 0 \pmod{\mathfrak{p}'}$ which is *not* true.

ART. **74.** We may next determine the congruence of least degree that is satisfied by the fundamental form ξ for the product $\mathfrak{p}\mathfrak{p}_1$ as modulus.

Suppose that

$$\Phi(\xi)\equiv 0 \pmod{\mathfrak{p}\mathfrak{p}_1},$$

where both $\mathfrak{p}$ and $\mathfrak{p}_1$ are ideal divisors of p, then, *a fortiori*

$$\Phi(\xi)\equiv 0 \pmod{\mathfrak{p}}.$$

Due to Lemma II of Art. 72

$$\Phi(x)\equiv\Pi(x)\Psi(x) \pmod{p}$$

and *a fortiori*

$$\Phi(\xi)\equiv\Pi(\xi)\Psi(\xi) \pmod{\mathfrak{p}\mathfrak{p}_1},$$

or

$$\frac{\Pi(\xi)}{\mathfrak{p}}\Psi(\xi)\equiv 0 \pmod{\mathfrak{p}_1}.$$

It follows that

$$\Psi(\xi)=0 \pmod{\mathfrak{p}_1}.$$

Due to Lemma II this requires that

$$\Psi(\xi)\equiv\Pi_1(\xi)\Phi_1(\xi) \pmod{\mathfrak{p}_1},$$

where the degree of Π_1 is the same as that of $\mathfrak{p}_1$.

With this is established the theorem: *The fundamental form ξ satisfies then and only then the congruence*

$$\Phi(\xi) \equiv 0 \pmod{\mathfrak{p}\mathfrak{p}_1},$$

if the congruence

$$\Phi(x) \equiv \Pi(x)\Pi_1(x)\Phi_1(x) \pmod{p}$$

exists; and that is, $\Phi(x)$ considered with respect to p, is divisible by $\Pi(x)\Pi_1(x)$.

An immediate consequence is the corollary: *The fundamental form ξ satisfies for the composite modulus $\mathfrak{p}\mathfrak{p}_1$ the congruence of least degree*

$$\Pi(x)\Pi_1(x) \equiv 0 \pmod{p},$$

whose degree is $f+f_1$, the sum of the degrees of $\mathfrak{p}$ and $\mathfrak{p}_1$.

ART. 75. We are now in a position to prove the following:

THEOREM I. *If the factorization of the rational prime integer p is expressed through*

$$p = \mathfrak{p}^e\mathfrak{p}_1^{e_1}\cdots,$$

the left hand side F of the fundamental equation is with respect to p factorable in the form

$$F(x) \equiv \Pi(x)^e\Pi_1(x)^{e_1}\cdots \pmod{p};$$

and, if we write

$$F(x) = \Pi(x)^e\Pi_1(x)^{e_1}\cdots + pG(x),$$

then $G(x)$ is an integral function in x; $u_1, u_2, \cdots, u_n$ with rational integral coefficients which is divisible by none of the prime functions $\Pi, \Pi_1, \cdots$. (Kronecker, *Grundzüge* § 25; Dedekind, *Werke*, Vol. I, pp. 202 ff.)

Proof. Let $\Phi(x)$ be an integral function of $x; u_1, \cdots, u_n$ with rational integral coefficients, such that the congruence $\Phi(x) \equiv 0 \pmod{p}$ is satisfied by the fundamental form ξ.

Observe next that the norm of

$$p = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots$$

is

$$p^n = p^{e_1 f_1 + e_2 f_2 + \cdots},$$

so that

$$n = e_1 f_1 + e_2 f_2 + \cdots.$$

Let $\Pi_1(x)$, $\Pi_2(x)$, $\cdots$ be the prime functions in x that are associated with the prime ideals $\mathfrak{p}$, $\mathfrak{p}_1$, $\cdots$, respectively. It follows then from the preceding article and Lemmas II and III of Art. 72 that

$$\Phi = \Pi^e \Pi_1^{e_1} \cdots \Psi \pmod{p},$$

where Ψ is an integral function like Φ. Since Π_1, Π_2, $\cdots$ are of degrees f_1, f_2, $\cdots$, it is seen that Φ must be of degree at least $e_1 f_1 + e_2 f_2 + \cdots = n$, and, this being the degree of the fundamental form F, we may write for Φ the function F.

With this is proved the first part of the theorem and at the same time it is a proof of the following:

THEOREM. *The congruence formed from the fundamental equation, namely,*

$$F(x; u_1, \cdots, u_n) \equiv 0 \pmod{p}$$

is the congruence of least degree with rational integral coefficients which is satisfied (mod. p), when for x is written the fundamental form ξ.

That $G(x)$ with respect to p is divisible by none of the functions, say $\Pi(x)$, is proved as follows:

Were $G(x)$ divisible by $\Pi(x)$, then $G(\xi)$ would be divisible by $\mathfrak{p}$, and it would follow from

$$F(\xi) \equiv 0 \equiv \Pi^e(\xi)\Pi^{e_1}(\xi) \cdots + pG(\xi)$$

that $\Pi^e(\xi)\Pi^{e_1}(\xi) \cdots$ is divisible by $\mathfrak{p}^{e+1}$, which is not true. From all this it follows that, if the fundamental equation written in the form of a congruence is

$$F(x) \equiv \Pi^e(x)\Pi^{e_1}(x) \cdots \pmod{p},$$

then is

$$p \sim (p + \Pi(\xi))^e (p + \Pi_1(\xi))^{e_1} \cdots.$$

And that is: If the content of $\Pi(\xi)$ is $(\alpha_1, \alpha_2, \cdots)$, that of

$\Pi_1(\xi)$ being $(\beta_1, \beta_2, \cdots)$, etc., then is

$$p=(p, \alpha_1, \alpha_2, \cdots)^e(p, \beta_1, \beta_2, \cdots)^{e_1}\cdots.$$

And with this it is seen that the *factorization of a prime rational integer into its prime ideal factors is made dependent upon the factorization, modulo p, of the fundamental form into its irreducible factors.*

For an example, see next chapter, Art. 99.

ART. 76. THEOREM. *The largest numerical factor of the discriminant of the fundamental equation is equal to the discriminant of the realm.* We write

$$(1)\qquad \begin{cases} 1=U_{11}\omega_1+U_{12}\omega_2+\cdots+U_{1n}\omega_n, \\ \xi=U_{21}\omega_1+U_{22}\omega_2+\cdots+U_{2n}\omega_n, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \xi^{n-1}=U_{n1}\omega_1+U_{n2}\omega_2+\cdots+U_{nn}\omega_n, \end{cases}$$

where the U's are integral functions of $u_1, u_2, \cdots, u_n$ with rational integral coefficients. The determinant U of (1) is a unit form. For, were it divisible by any prime integer p, it would be possible (Vol. I, Art. 56) to determine n functions $V_1, V_2, \cdots, V_n$, such that

$$(2)\qquad V_1U_{1i}+V_2U_{2i}+\cdots+V_nU_{ni}\equiv 0 \pmod{p} \qquad (i=1, 2, \cdots, n).$$

It would follow immediately from (1) that

$$V_1+V_2\xi+\cdots+V_n\xi^{n-1}\equiv 0 \pmod{p}.$$

It was shown above, however, that ξ does not satisfy any congruence (mod. p) of degree less than n. It follows at once from the relations (1) that

$$\begin{vmatrix} 1, & \xi, & \cdots, & \xi^{n-1} \\ 1, & \xi', & \cdots, & \xi'^{n-1} \\ \cdots & \cdots & \cdots & \cdots \\ 1, & \xi^{(n-1)}, & \cdots, & (\xi^{(n-1)})^{n-1} \end{vmatrix} = U \begin{vmatrix} \omega_1, & \omega_2, & \cdots, & \omega_n \\ \omega_1', & \omega_2', & \cdots, & \omega_n' \\ \cdots & \cdots & \cdots & \cdots \\ \omega_1^{(n-1)}, & \omega_2^{(n-1)}, & \cdots, & \omega_n^{(n-1)} \end{vmatrix}.$$

If both sides of this expression are squared, it is seen that

$$\Delta(\xi)=U^2D \qquad \text{or} \qquad \Delta(\xi)\simeq D,$$

where D is the discriminant of the realm, the basal invariant of Vol. I, Art. 94. With this is proved by Hensel (*op. cit.*, p. 78) the theorem conjectured by Kronecker (*Grundzüge*, p. 113) that the discriminant of the fundamental equation of any realm is in absolute value equivalent to the discriminant of the realm; and that is, both have the same rational integral divisors.

In this manner Kronecker "would reduce the entire arithmetical theory of algebraic numbers to a theory of integral functions of variables and indeterminates with rational integral coefficients."

Finally, observe that from the relations (1) the quantities ω_i may be expressed as integral functions of degree $n-1$ in ξ, with coefficients that are integral in $u_1, \cdots, u_n$ divided by the unit form U. And, as every integer γ of the realm is of the form

$$\gamma = a_1\omega_1 + \cdots + a_n\omega_n,$$

where the a's are rational integers, it follows that every such integer γ is equal to $\dfrac{g(\xi; u_1, \cdots, u_n)}{U}$, where g is an integral function of the $n-1$ degree in ξ with coefficients that are integral functions of $u_1, \cdots, u_n$ with rational integral coefficients.

ART. **77.** A further consequence as given by Hilbert (p. 200 of his *Bericht*) is added here.

He called the $n-1$ ideals

$$\begin{aligned}
\mathfrak{e}' &= ((\omega_1-\omega_1'), \cdots, (\omega_n-\omega_n')),\\
\mathfrak{e}'' &= ((\omega_1-\omega_1''), \cdots, (\omega_n-\omega_n'')),\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
\mathfrak{e}^{(n-1)} &= ((\omega_1-\omega_1^{(n-1)}), \cdots, (\omega_n-\omega_n^{(n-1)})),
\end{aligned}$$

the $n-1$ *elements* of the realm in which $\mathfrak{o} = (\omega_1, \omega_2, \cdots, \omega_n)$ is the order-modul. In general these ideals do not belong to the realm in which Hilbert defines them as

elements. Observe, however, that the product of the elements $\mathfrak{e}', \mathfrak{e}'', \cdots, \mathfrak{e}^{(n-1)}$ is an ideal of the fixed realm. The elements are the contents of the forms $\xi-\xi', \cdots, \xi-\xi^{(n-1)}$. Hilbert defines the ideal $\mathfrak{d}=\mathfrak{e}\cdot\mathfrak{e}\cdots\mathfrak{e}^{(n-1)}=\mathfrak{d}(\xi)$ as the *different*[1] (Vol. I, Art. 96) of the fundamental form, and that is

$$\mathfrak{d}(\xi)=\left[\frac{\partial F}{\partial x}\right]_{x=\xi}=(\xi-\xi')(\xi-\xi'')\cdots(\xi-\xi^{(n-1)}),$$

which is a quantity of the fixed realm. The norm of this different is equal to the greatest numerical factor of the discriminant of the fundamental form, which from above is equal to the discriminant of the realm; and that is,

$$|N(\mathfrak{d}(\xi))|=|\Delta(\xi)|=|U^2D|.$$

$\mathfrak{d}(\xi)$ is sometimes called the *fundamental* ideal of the realm. (See foot-note in Art. 106.) From the congruence

$$\frac{\partial F(x)}{\partial x}\equiv e\Pi^{e-1}\frac{\partial\Pi}{\partial x}\Pi_1^{e_1}\cdots+e_1\frac{\partial\Pi_1}{\partial x}\Pi^{e}\Pi_1^{e_1-1}\cdots+\cdots\ (\text{mod. } p),$$

it is seen that the different $\mathfrak{d}(\xi)$ is divisible by $\mathfrak{p}^{e-1}$ and that this different is divisible by no higher power of $\mathfrak{p}$, if the exponent e is relatively prime to $\mathfrak{p}$. If the norm of this expression is taken, it is clear that the discriminant of the realm is always divisible by

$$p^{f(e-1)+f_1(e_1-1)+\cdots},$$

and by no higher power of p, if all the exponents $e, e_1, \cdots,$ are relatively prime[2] to p. With this is again (Art. 31) proved the theorem: *The discriminant of a fixed realm contains all and only those rational prime integers as factors which are divisible by the square of a prime ideal.*

[1] The *different* of a realm is treated by Ö. Ore, *Acta Math.*, Vol. 46, pp. 365 ff.

[2] For the case where one of the e's is divisible by p see Art. 92.

CHAPTER V

THE CONTRIBUTIONS OF HURWITZ

ART. **78.** In Art. 14 it was seen that if the ideal $\mathfrak{c}$ is divisible by the ideal $\mathfrak{a}$, there exists another ideal $\mathfrak{b}$ such that

(1) $$\mathfrak{c} = \mathfrak{a}\mathfrak{b}.$$

It was also shown that this result follows at once, if it be proved that given any ideal $\mathfrak{i}$, another ideal $\mathfrak{i}_1$ may be found such that

$$\mathfrak{i}\mathfrak{i}_1 = \mathfrak{o}\gamma,$$

where γ is an integer in the fixed realm and where $\mathfrak{o}$ the order-modul consists of all the integers of this realm; and that is, the product $\mathfrak{i}\mathfrak{i}_1$ is equal to a principal ideal in the fixed realm.

Hurwitz [1] in his treatment of ideal makes the proof of the latter theorem fundamental. The proof of Hurwitz is an extension of the Theorem of Gauss (see Vol. I, Art. 4). In its reproduction I have followed Humbert. See Note I of the appendix of the Translation by Levy and Got of Hilbert's "Bericht über die Theorie der algebraischen Zahlkörper," *Jahresber. der deutsch. Mathematiker-Vereinigung*, 1894–95.

Extension [2] *of the Theorem of Art. 15 as stated by Gauss with a Proof of the Primary Theorem of Art. 14.*

[1] See *Nachrichten von der Königl. Gesellschaft d. Wissenschaften zu Göttingen*, 1894, p. 291. In a footnote to this article Hurwitz says that he was unaware of a proof of Dedekind of the same theorem in 1892. See Art. 14 of the present work. See also p. 272 of the volume of the *Nachrichten* just cited for the statement by Dedekind that as far back as 1869–70 he had succeeded in overcoming the "last difficulties."

[2] See Kronecker, *Werke*, Vol. I, p. 109; Mertens, *Ber. d. K. Akad. der Wiss. zu Wien*, 1892; and *Wiener Sitzber.*, 1894, p. 6; J. König, *Einleitung in die allgemeine Theorie der algebraischen Grössen*, 1903, pp. 74 et seq.

THEOREM. *Let*

$$F(x)=\alpha_0x^m+\alpha_1x^{m-1}+\cdots+\alpha_m,$$

and

$$G(x)=\beta_0x^n+\beta_1x^{n-1}+\cdots+\beta_n,$$

be two polynomials in x, whose coefficients are algebraic integers; and let

$$F(x)G(x)=\gamma_0x^{m+n}+\gamma_1x^{m+n-1}+\cdots+\gamma_{m+n};$$

if further each of the γ's is divisible by the algebraic integer ω, then is each of the products $\alpha_i\beta_k$ ($i=0, 1, 2, \cdots, m$; $k=0, 1, \cdots, n$) divisible by ω. And that is, if $\frac{\gamma_h}{\omega}$ ($h=0, 1, 2, \cdots, m+n$) are algebraic integers, then also $\frac{\alpha_i\beta_k}{\omega}$ ($i=0, 1, 2, \cdots, m$; $k=0, 1, 2, \cdots, n$) are algebraic integers.

Denote the roots of the function $F(x)$ by $x_1, x_2, \cdots, x_m$, and let the roots of $G(x)$ be $y_1, y_2, \cdots, y_n$. If S indicates a symmetric function of the quantities that follow it, we have

$$\pm\frac{\alpha_i}{\alpha_0}\frac{\beta_k}{\beta_0}=S(x_1, x_2, \cdots, x_i)S(y_1, y_2, \cdots, y_k).$$

Let i and k be fixed. Next let $\xi_1, \xi_2, \cdots, \xi_{m+n}$ be the roots of the equation $F(x)G(x)=0$, being the quantities $x_1, x_2, \cdots, x_m; y_1, y_2, \cdots, y_n$ without regard to their order. Distribute the ξ's in every possible manner into two groups such that in the one group there are m quantities and n in the second. In any such distribution let $\zeta_1, \zeta_2, \cdots, \zeta_m$ be the quantities of the one group and $\eta_1, \eta_2, \cdots, \eta_n$ those of the other group. Note that the function $u=(\sum\zeta_1\zeta_2\cdots\zeta_i)(\sum\eta_1\eta_2\cdots\eta_k)$ is not a *symmetric function* of the ξ's. In making all possible distribution of $\xi_1, \xi_2, \cdots, \xi_{m+n}$ into two groups of m and n, respectively, there results a certain number of functions u, of which one is $(\sum x_1x_2\cdots x_i)(\sum y_1y_2\cdots y_k)$, and that is

$\pm\frac{\alpha_i}{\alpha_0}\cdot\frac{\beta_k}{\beta_0}$. Note, however, that every symmetric function of the u's is also a symmetric function of the ξ's. Hence the u's are the roots of an algebraic equation, whose coefficients are polynomials in $\frac{\gamma_i}{\gamma_0}$ $[i=0, 1, \cdots, m+n]$.

Observe that, if

$$t^k+c_1t^{k-1}+c_2t^{k-2}+\cdots+c_k=0$$

is an equation with roots $t_1, t_2, \cdots, t_k$, any symmetric function $S(t_1^{a_1}, \cdots, t_i^{a_i})$ $[i=1, \cdots, k]$, the a's being positive integers or zero, may be expressed as a polynomial in $c_1, c_2, \cdots, c_k$, with integral coefficients, whose degree is that of the greatest of the a's.

Let

$$u^M+d_1u^{M-1}+\cdots+d_M=0 \qquad \text{(i)}$$

be the equation in u. Then is

$$-d_1=S(\sum(\zeta_1\zeta_2\cdots\zeta_i)\sum(\eta_1\eta_2\cdots\eta_k)).$$

As the ξ's occur only to the *first* degree in this symmetric function, it is seen that d_1 is a polynomial of the first degree in $\frac{\gamma_i}{\gamma_0}$ $[i=1, 2, \cdots, m+n]$. Similarly, d_2 is a polynomial of the second degree in the quantities $\frac{\gamma_i}{\gamma_0}$, etc.

We may therefore write the equation (i) in the form

$$u^M+\frac{P_1}{\gamma_0}u^{M-1}+\frac{P_2}{\gamma_0^2}u^{M-2}+\cdots+\frac{P_M}{\gamma_0^M}=0,$$

where P_i $[i=1, \cdots, M]$ are polynomials with rational integral coefficients of degrees i in the quantities $\gamma_0, \gamma_1, \cdots, \gamma_{m+n}$ and *homogeneous*. It was seen that $\frac{\alpha_i}{\alpha_0}\cdot\frac{\beta_k}{\beta_0}$ was one of the u's and therefore satisfies the above equation. Hence, writing $\alpha_i\beta_k=v$, and observing that

$\alpha_0\beta_0=\gamma_0$, it is seen that v satisfies the equation

$$\left(\frac{v}{\gamma_0}\right)^M+\frac{P_1}{\gamma_0}\left(\frac{v}{\gamma_0}\right)^{M-1}+\cdots+\frac{P_M}{\gamma_0^M}=0,$$

and that is

$$v^M+P_1v^{M-1}+\cdots+P_M=0.$$

This last equation may be written in the form

$$\left(\frac{v}{\omega}\right)^M+\frac{P_1}{\omega}\left(\frac{v}{\omega}\right)^{M-1}+\frac{P_2}{\omega^2}\left(\frac{v}{\omega}\right)^{M-2}+\cdots+\frac{P_M}{\omega^M}=0. \quad \text{(ii)}$$

Since by hypothesis each of the γ's is divisible by ω, it is clear that the coefficients $\frac{P_\nu}{\omega^\nu}$ $[\nu=1, \cdots, M]$ are algebraic integers, and hence (Vol. I, Art. 88) $\frac{v}{\omega}$ the root of (ii) is an algebraic integer; and that is, $\frac{\alpha_i\beta_k}{\omega}$ $(i=1, 2, \cdots, m;$ $k=1, 2, \cdots, n)$ are algebraic integers. With this is proved, what we called (Art. 15) the *Generalized Gaussian Theorem.*

It is easy to derive from this the *Primary Theorem*, namely: *For any definite ideal* $\mathfrak{i}=(\alpha_1, \alpha_2, \cdots, \alpha_n)$ *another ideal* $\mathfrak{i}_1$ *may be found such that the product* $\mathfrak{i}\mathfrak{i}_1$ *is a principal ideal.*

For, write

$$\xi=\alpha_1u_1+\alpha_2u_2+\cdots+\alpha_nu_n,$$

and denote the product of the $n-1$ conjugate forms by

$$\begin{aligned}\Pi=\prod_{i=1}^{i=n-1}(\xi^{(i)})&=(\alpha_1^{(1)}u_1+\alpha_2^{(1)}u_2+\cdots+\alpha_n^{(1)}u_n)\\&\times(\alpha_1^{(2)}u_1+\cdots+\alpha_n^{(2)}u_n)(\alpha_1^{(n-1)}u_1+\cdots+\alpha_n^{(n-1)}u_n)\\&=\beta_1U_1+\beta_2U_2+\cdots+\beta_sU_s,\end{aligned}$$

where the β's are algebraic integers that belong to the same realm as do $\alpha_1, \alpha_2, \cdots, \alpha_n$, and the U's are integral functions of $u_1, \cdots, u_n$. Observe that

$$\Pi\cdot F=gU,$$

where g is a rational integer and U an integral function of the u's with rational integral coefficients, whose greatest common divisor is unity. It follows on the one hand that g is divisible by the product of the contents of Π and F, and that is, by $\mathfrak{i}$ and $\mathfrak{i}_1$, where $\mathfrak{i}_1 = (\beta_1, \beta_2, \cdots, \beta_s)$; and on the other hand, due to the above lemma, $\alpha_i\beta_h$ is divisible by g and that is $\mathfrak{i}\mathfrak{i}_1$ is divisible by g. It follows that

$$\mathfrak{o}g = \mathfrak{i}\mathfrak{i}_1.$$

ART. **79.** With the above theorem Hurwitz wished to establish the general theory of ideals by proving the following theorems. As these theorems have all been well established in the preceding Dedekind or Kronecker theories, we shall introduce them again in a synoptic form as they were given by Hurwitz:

THEOREM. *If the three ideals* $\mathfrak{a}$, $\mathfrak{b}$ *and* $\mathfrak{c}$ *satisfy the equation* $\mathfrak{a}\mathfrak{c} = \mathfrak{b}\mathfrak{c}$, *then is* $\mathfrak{a} = \mathfrak{b}$. For, let the ideal $\mathfrak{c}_1$ satisfy the relation $\mathfrak{c}\mathfrak{c}_1 = \mathfrak{o}g$. Then due to the relation $\mathfrak{a}\mathfrak{c}\mathfrak{c}_1 = \mathfrak{b}\mathfrak{c}\mathfrak{c}_1$, it follows that $\mathfrak{a}g = \mathfrak{b}g$, or $\mathfrak{a} = \mathfrak{b}$.

DEFINITION. An ideal $\mathfrak{c}$ is said to be *divisible* by an ideal $\mathfrak{a}$, if there is another ideal $\mathfrak{b}$ such that $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$. Since $\mathfrak{a} = \mathfrak{a}\mathfrak{o}$, every ideal is divisible by itself and by $\mathfrak{o}$.

DEFINITION. An ideal that is different from $\mathfrak{o}$ and which is only divisible by itself and by $\mathfrak{o}$, is a *prime ideal.*

THEOREM. *If all the integers of the ideal* $\mathfrak{c}$ *are divisible by the ideal* $\mathfrak{a}$, *then is* $\mathfrak{c} > \mathfrak{a}$.

For, write $\mathfrak{a}\mathfrak{a}_1 = \mathfrak{o}a$ and observe that all the integers of $\mathfrak{a}_1\mathfrak{c}$ are divisible by $\mathfrak{a}\mathfrak{a}_1$ and that is by a. Hence, there exists an ideal $\mathfrak{b}$ such that $\mathfrak{a}_1\mathfrak{c} = a\mathfrak{b}$ and therefore also $\mathfrak{a}\mathfrak{a}_1\mathfrak{c} = a\mathfrak{a}\mathfrak{b}$ or $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$. Obviously this is another form of the *Primary Theorem.*

THEOREM. *If* $\mathfrak{a}\mathfrak{a}_1 = \mathfrak{o}$, *then is* $\mathfrak{a} = \mathfrak{o} = \mathfrak{a}_1$; for $\mathfrak{o}$ is only divisible by $\mathfrak{o}$.

THEOREM. *Every ideal* $\mathfrak{a}$ *has only a finite number of divisors.* For as above, let $\mathfrak{b}$ be an ideal such that $\mathfrak{ab} = a\mathfrak{o}$, where a is a positive rational integer. It follows that a is an element of every ideal, that is a divisor of $\mathfrak{a}$. And there is only a finite number of such ideals (Art. 25).

THEOREM. *If* $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2$ *and if* $\mathfrak{a}_2$ *is different from* $\mathfrak{o}$, *then* $\mathfrak{a}_1$ *has fewer divisors than* $\mathfrak{a}$. For if $\mathfrak{d}_1, \mathfrak{d}_2, \cdots, \mathfrak{d}_k$ are the divisors of $\mathfrak{a}_1$, then the ideal $\mathfrak{a}$ has the divisors

$$\mathfrak{d}_1, \mathfrak{d}_2, \cdots, \mathfrak{d}_k \quad \text{and} \quad \mathfrak{d}_1\mathfrak{a}_2, \mathfrak{d}_2\mathfrak{a}_2, \cdots, \mathfrak{d}_k\mathfrak{a}_2;$$

and were the last k divisors the same as the first, it would follow that

$$\mathfrak{d}_1\mathfrak{a}_2 \cdot \mathfrak{d}_2\mathfrak{a}_2 \cdots \mathfrak{d}_k\mathfrak{a}_2 = \mathfrak{d}_1\mathfrak{d}_2 \cdots \mathfrak{d}_k \quad \text{or} \quad \mathfrak{a}_2^k = \mathfrak{o}.$$

It follows that $\mathfrak{a}_2 = \mathfrak{o}$, contrary to the hypothesis. Accordingly, it is seen that an ideal can have only a finite number of factors.

THEOREM. *If the product of two ideals* $\mathfrak{ab}$ *is divisible by the prime ideal* $\mathfrak{p}$, *then is one of these ideals divisible by* $\mathfrak{p}$. For, if $\mathfrak{a}$ is not divisible by $\mathfrak{p}$, the greatest common divisor of $\mathfrak{a}$ and $\mathfrak{p}$ is $\mathfrak{o}$ by the definition of a prime ideal, or $\mathfrak{a} + \mathfrak{p} = \mathfrak{o}$. It follows that $1 = \alpha + \pi$, where α is an integer of $\mathfrak{a}$ and π one of $\mathfrak{p}$. Multiplying this expression by any arbitrary integer β of $\mathfrak{b}$, it is seen that $\beta = \alpha\beta + \pi\beta$. And as $\alpha\beta$ and $\pi\beta$ are both divisible by $\mathfrak{p}$, it follows that β, and therefore from one of the preceding theorems, that $\mathfrak{b}$ is divisible by $\mathfrak{p}$.

From this follows the *Fundamental Theorem*, viz., *the factorization of an ideal into its prime ideal factors is a unique process.* For if $\mathfrak{a}$ is not a prime ideal, it may be written $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2$, where $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are different from $\mathfrak{a}$ and from $\mathfrak{o}$. And from above the number of divisors of both $\mathfrak{a}_1$ and $\mathfrak{a}_2$ is less than that of $\mathfrak{a}$. If one of the ideals $\mathfrak{a}_1$ and $\mathfrak{a}_2$ is not a prime ideal it may be factored as was done with $\mathfrak{a}$, etc. Since the number of divisors of such

ideals becomes smaller, the factorization must finally end in a product of prime ideal factors. It follows also as in Art. 27 that such a factorization is unique.

ART. **80.** The theorem of Kronecker that *the content of the product of two forms is equal to the product of their contents, is derived* as follows by Hurwitz:

If φ, ψ, $\cdots$ are integral functions of the variables x_1, x_2, $\cdots$, x_k, they may be transformed through the substitutions

$$x_1 = x'^{t_1},\ x_2 = x'^{t_2},\ \cdots,\ x_k = x'^{t_k}$$

into integral functions Φ, Ψ, $\cdots$, of x; and the positive integers $t_1, t_2, \cdots, t_k$ may be so chosen that the number of terms that are found in φ, ψ, $\cdots$ is the same as that in Φ, Ψ, $\cdots$, so that the coefficients of φ are the same as those of Φ, those of ψ being the same as those of Ψ, etc.

The Generalized Gaussian Theorem is at once applicable and may be stated as follows:

If φ and ψ are rational integral functions of any number of variables with integral algebraic coefficients, and if each coefficient in the product $\varphi\psi$ is divisible by the algebraic integer ω, then ω divides every product that is formed by a coefficient of φ and one of ψ.

A repetition of this theorem offers a further generalization:

If φ, ψ, χ, $\cdots$ are rational integral functions in any number of variables with integral algebraic coefficients, and if each coefficient of the product $\varphi\psi\chi\cdots$ is divisible by the algebraic integer ω, then is also every term made of the product of a coefficient of each of the functions φ, ψ, χ, $\cdots$, divisible by ω.

Next suppose that φ_1 and φ_2 are integral rational functions in any number of variables with coefficients, respectively, $\alpha_1^{(1)}$, $\alpha_2^{(1)}$, $\cdots$, $\alpha_1^{(2)}$, $\alpha_2^{(2)}$, $\cdots$, and let α_1, α_2, $\cdots$ be the coefficients of the product $\varphi = \varphi_1\varphi_2$.

The Kronecker Theorem is: *The product of the ideals*

$$\mathfrak{a}_1 = (\alpha_1^{(1)}, \alpha_2^{(1)}, \cdots), \qquad \mathfrak{a}_2 = (\alpha_1^{(2)}, \alpha_2^{(2)}, \cdots)$$

is equal to the ideal

$$\mathfrak{a} = (\alpha_1, \alpha_2, \cdots). \qquad \text{(See Art. 68.)}$$

In fact, if (Art. 69) ψ denotes the product of the functions that are conjugate to φ and if $\beta_1, \beta_2, \cdots$ are the coefficients of φ, then is $\varphi\psi = \varphi_1\varphi_2\psi = \Phi$, where Φ is the norm of φ.

If the rational integer a is the greatest common divisor of the coefficients of Φ, it follows from the two theorems just stated that

$$\mathfrak{a}\mathfrak{b} = (a) \qquad \text{and} \qquad \mathfrak{a}_1\mathfrak{a}_2\mathfrak{b} = (a),$$

where $\mathfrak{b}$ denotes the ideal $(\beta_1, \beta_2, \cdots)$; and from these two relations it follows that

$$\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2.$$

ART. 81. Another proof of the Primary Theorem was given by Hurwitz in the *Göttingen Nachrichten*, 1895, p. 324. As it depends upon a method which has been emphasized in the present treatise, it will be presented here.

LEMMA. *If τ is an arbitrary number of a fixed realm $\Re(\theta)$ of degree n, an algebraic integer μ of this realm and a positive rational integer h may be so determined that the norm of the number $h\tau - \mu$ is in absolute value less than 1; and h is not greater than a positive integer m which does not depend upon τ but upon the fixed realm.*

Let $\omega_1, \omega_2, \cdots, \omega_n$ be any integral basis of the realm, so that

$$\tau = r_1\omega_1 + r_2\omega_2 + \cdots + r_n\omega_n,$$

where the r's are rational numbers. Further let k be a positive integer to be determined later, and for each of the k^n+1 integers

$$i = 0, 1, 2, 3, \cdots, k^n$$

determine the algebraic integer

$$\mu_i = g_1\omega_1 + g_2\omega_2 + \cdots + g_n\omega_n,$$

the g's being rational integers and such that the coefficients in the number

(1) $$i\tau - \mu_i = (ir_1 - g_1)\omega_1 + (ir_2 - g_2)\omega_2 + \cdots + (ir_n - g_n)\omega_n$$

shall be contained between 0 inclusive and 1 exclusive.

Divide the interval from 0 to 1 into k equal parts

$$0 \cdots \frac{1}{k}, \frac{1}{k} \cdots \frac{2}{k}, \cdots, \frac{k-1}{k} \cdots k,$$

and as belonging to each interval count the lower limit, and let the upper limit be counted as belonging to the following interval. As there are in the formula (1) n coefficients and as each coefficient may fall within one of the k intervals, there are in all k^n possible distributions for these coefficients. As there are, however, k^n+1 values of i, it is seen that for two of these values the coefficients of the quantities $i\tau - \mu_i$ must fall within the same intervals. If the difference of these two quantities is denoted by

$$h\tau - \mu = d_1\omega_1 + d_2\omega_2 + \cdots + d_n\omega_n,$$

it is seen that $d_i\,[i = 1, 2, \cdots, n]$ are numerically less than $\frac{1}{k}$, while h is one of the integers $1, 2, \cdots, k^n$.

It follows that the absolute value of $h\tau - \mu$ is not greater than $\frac{1}{k}$ times the sum of the absolute values of $\omega_1, \omega_2, \cdots, \omega_n$. Denote this sum by ω. If Ω denotes the largest of the absolute values of the conjugates of ω, it is seen that $N(h\tau - \mu)$ is less than $\frac{1}{k^n}\Omega^n$, where Ω depends *only* upon the fixed realm. If next the integer k is chosen greater than Ω, it is clear that $|h\tau - \mu| < 1$, where h is

not greater than $k^n = m$, say. With this the lemma is proved.

ART. 82. Let i be an arbitrary ideal of the realm and let α be any integer of i. Further suppose that the norm of α, say a, is the smallest rational integer that is divisible by i, so that no other integer is found in i whose norm is less than a. If α' is any other integer of i, it is seen through applying the above lemma to the number $\tau = \frac{\alpha'}{\alpha}$, that there is a number $h\alpha' - \mu\alpha$, whose norm is less than a. It follows that

$$N(h\alpha' - \mu\alpha) = 0, \qquad \text{or} \qquad h\alpha' = \mu\alpha.$$

And that is, $h\alpha'$ is divisible by α.

Since h is one of the integers $1, 2, 3, \cdots, m$, it is clear, if we put $M = 1 \cdot 2 \cdot 3 \cdots m$, that every number of the ideal Mi is divisible by α. The complex of these numbers form an ideal αi', where i' is an ideal of the fixed realm.

It follows that

(1) $$M\mathfrak{i} = \alpha\mathfrak{i}',$$

and with it the equivalence of the ideals i and i'. Since α is a number in i, it is seen from this relation that M is a number in i'. There are however only a finite number of ideals (Art. 25) in which M may appear as an element. With this it is proved that every ideal i is equivalent to an ideal in which M enters as an element. There being only a finite number of such ideals, it follows that there is only a finite number of inequivalent classes of ideals.

ART. 83. If h denotes this finite number of classes, it is evident that among the $h+1$ ideals

$$\mathfrak{i}, \mathfrak{i}^2, \mathfrak{i}^3, \cdots, \mathfrak{i}^{h+1},$$

there must be at least two equivalent to each other. If these are $\mathfrak{i}^r$ and $\mathfrak{i}^s$, where $s > r$, it follows that

$$\gamma'\mathfrak{i}^r = \gamma''\mathfrak{i}^s,$$

where γ' and γ'' are two integers of the realm. This equation may be written

$$\gamma \mathfrak{i}^r = \mathfrak{i}^r \mathfrak{i}^{s-r}, \tag{1}$$

where

$$\gamma = \frac{\gamma'}{\gamma''}.$$

Denote by

$$\alpha_1, \alpha_2, \cdots, \alpha_n; \beta_1, \beta_2, \cdots, \beta_n,$$

the bases of $\mathfrak{i}^r$ and $\mathfrak{i}^{s-r}$, respectively. It follows from (1) on the one hand that the numbers $\gamma\alpha_1, \gamma\alpha_2, \cdots, \gamma\alpha_n$ are linear homogeneous expressions in $\alpha_1, \alpha_2, \cdots, \alpha_n$ with coefficients that belong to $\mathfrak{i}^{s-r}$ and are accordingly algebraic integers.

If the ξ's denote algebraic integers, it is also seen by writing

$$\gamma\alpha_i = \alpha_1\xi_{i1} + \alpha_2\xi_{i2} + \cdots + \alpha_n\xi_{in} \quad (i = 1, 2, \cdots, n),$$

that γ is an integer of the realm.

It follows further from (1) that

$$\beta_i\alpha_1, \beta_i\alpha_2, \cdots, \beta_i\alpha_n \qquad (i = 1, 2, \cdots, n)$$

are linear homogeneous expressions in $\gamma\alpha_1, \gamma\alpha_2, \cdots, \gamma\alpha_n$, with integral coefficients, and accordingly $\frac{\beta_i}{\gamma} = \gamma_i$, say, $(i = 1, \cdots, n)$ are integers of the realm.

If $\mathfrak{i}' = (\gamma_1, \gamma_2, \cdots, \gamma_n)$, then is

$$\mathfrak{i}^{s-r} = \gamma\mathfrak{i}'. \tag{2}$$

And from (1) it is seen that $\mathfrak{i}^r = \mathfrak{i}^r\mathfrak{i}'$, and accordingly

$$1 \cdot \alpha_i = \alpha_1\tau_{i1} + \alpha_2\tau_{i2} + \cdots + \alpha_n\tau_{in} \quad (i = 1, 2, \cdots, n),$$

the τ's bring algebraic integers, and therefore 1 is an integer in $\mathfrak{i}'$, so that (Art. 58) $\mathfrak{i}' = \mathfrak{o}$.

From (2) we have

$$\mathfrak{i}^{s-r} = \mathfrak{o}\gamma;$$

and that is: belonging to *every ideal* $\mathfrak{i}$ *there is a certain power, say* k, *such that* $\mathfrak{i}^k$ *is a principal ideal.* If further

$k>1$, then $\mathfrak{i}_1(=\mathfrak{i}^{k-1})$ is an ideal such that $\mathfrak{i}\mathfrak{i}_1$ is a principal ideal. For $k=1$, and that is, when $\mathfrak{i}$ is itself a principal ideal, then $\mathfrak{i}_1=\mathfrak{o}$. With this the *Primary Theorem* is proved anew.

ART. **84.** Further consequences may be drawn: *If* $\mathfrak{i}^k$ *is the lowest power of* $\mathfrak{i}$, *which is a principal ideal, then* k *must be a divisor of* h. Evidently the ideals

$$\mathfrak{i},\ \mathfrak{i}^2,\ \cdots,\ \mathfrak{i}^k, \tag{1}$$

are not equivalent. For, from the equivalence of any two of these ideals would follow that a lower power of $\mathfrak{i}$ was a principal ideal. If $k<h$, there must be an ideal $\mathfrak{i}_1$ which is equivalent to none of the ideals (1). It may be proved that the ideals

$$\mathfrak{i}_1\mathfrak{i},\ \mathfrak{i}_1\mathfrak{i}^2,\ \cdots,\ \mathfrak{i}_1\mathfrak{i}^k, \tag{2}$$

are not equivalent either to (1) or to one another. Were any two of the ideals (2) equivalent, it would follow also that two of the ideals (1) were equivalent. For, were $\omega'\mathfrak{i}_1\mathfrak{i}^r=\omega''\mathfrak{i}_1\mathfrak{i}^s$, and were $\mathfrak{i}_1\mathfrak{i}'=$ a principal ideal, say $\tau\mathfrak{o}$, it would follow by multiplying by $\mathfrak{i}'$, that $\omega'\mathfrak{i}^r=\omega''\mathfrak{i}^s$.

If $\omega'\mathfrak{i}_1\mathfrak{i}^r=\omega''\mathfrak{i}^s$, and if $\mathfrak{i}^k$ is a principal ideal $\mathfrak{o}\gamma$, it follows through multiplying by $\mathfrak{i}^{k-r}$ that $\omega'\gamma\mathfrak{i}_1=\omega''\gamma\mathfrak{i}^{s-r}$, from which follows the equivalence of $\mathfrak{i}_1$ with one of the ideals (1).

Accordingly h is at least equal to $2k$. If $h>2k$, there exists an ideal $\mathfrak{i}_2$ which is different from the ideals (1) and (2). Forming the ideals

$$\mathfrak{i}_2\mathfrak{i},\ \mathfrak{i}_2\mathfrak{i}^2,\ \cdots,\ \mathfrak{i}_2\mathfrak{i}^k, \tag{3}$$

it may be proved that none of these ideals is equivalent to the ideals (1), or (2), nor is it equivalent to any of the ideals (3) excepting of course itself.

Continuing in this manner, it is clear that h is some multiple of k. Since $\mathfrak{i}^k$ is a principal ideal, we have the theorem:

If h is the number of classes of non-equivalent ideals, the h-power of every ideal is a principal ideal, and that is

$$\mathfrak{i}^h = \mathfrak{o}\gamma.$$

Since the class to which the product of two ideals belong is the product of the classes to which these ideals belong, the theorems proved above for ideals are at once applicable to the classes. Since these results are the same as those found in Art. 52, they will not be repeated here.

ART. **85.** As an analog for the theorem relative to the greatest common divisor of rational integers, Hurwitz [1] offers the following. It is in a manner an *existence-proof* of the greatest common divisor of algebraic integers:

If $\alpha_1, \alpha_2, \cdots, \alpha_r$ are any algebraic integers, it was seen (Vol. I, Art. 51), that

$$\Re(\alpha_1, \alpha_2, \cdots, \alpha_r) = \Re(\alpha),$$

say, is a realm in which they all belong. Let h be the number of classes in $\Re(\alpha)$ and observe that

$$\mathfrak{i} = (\alpha_1, \alpha_2, \cdots, \alpha_r)$$

is an ideal in this realm.

Further, since

$$\mathfrak{i}^h = (\alpha_1, \alpha_2, \cdots, \alpha_r)^h = \mathfrak{o}\gamma, \qquad (a)$$

it is seen that each of the integers $\alpha_1^h, \alpha_2^h, \cdots, \alpha_r^h$, is divisible by γ, and therefore $\alpha_1, \alpha_2, \cdots, \alpha_r$ are each divisible by $\sqrt[h]{\gamma} = \gamma_0$, where γ_0 is an algebraic integer (Vol. I, Art. 88). It follows that γ_0 is a common divisor of $\alpha_1, \alpha_2, \cdots, \alpha_r$, and every divisor of γ_0 is a common divisor of these integers.

It follows also from (a) that the integer γ is a homogeneous function of the hth dimension in the quantities $\alpha_1, \alpha_2, \cdots, \alpha_r$, with integral algebraic coefficients, and

[1] *Göttinger Nachr.*, 1895, Heft, 3.

may be written in the form

$$\gamma=\alpha_1\beta_1+\alpha_2\beta_2+\cdots+\alpha_r\beta_r,$$

where the β's are homogeneous function of the $h-1$ degree in the α's with integral coefficients in $\Re(\alpha)$. It is seen that if $\mathfrak{d}$ is a common divisor of $\alpha_1, \alpha_2, \cdots, \alpha_r$, that $\mathfrak{d}^h$ is a divisor of $\gamma=\gamma_0^h$, and accordingly $\mathfrak{d}$ is a divisor of γ_0. With this, it is seen that the common divisors of $\alpha_1, \alpha_2, \cdots, \alpha_r$ are divisors of γ_0.

Further, from above

$$\gamma_0^h=\alpha_1\beta_1+\alpha_2\beta_2+\cdots+\alpha_r\beta_r,$$

where

$$\beta_i=\gamma_0^{h-1}\gamma_i \qquad (i=1, 2, \cdots, r),$$

so that

$$\gamma_0=\alpha_1\gamma_1+\alpha_2\gamma_2+\cdots+\alpha_r\gamma_r, \qquad (b)$$

where $\gamma_1, \gamma_2, \cdots, \gamma_r$ are integers which like γ_0 do not in general belong to the fixed realm $\Re(\alpha)$.

It is thus proved that *for any given algebraic integers* $\alpha_1, \alpha_2, \cdots, \alpha_r$, *there is always an algebraic integer* γ_0 *of the form* (*b*) *and such that all its divisors are identical with those divisors that are common to the given integers.*

Hurwitz wished to consider γ_0 the *greatest common divisor* of $\alpha_1, \alpha_2, \cdots, \alpha_r$. If γ_0 were an algebraic unit, the integers $\alpha_1, \alpha_2, \cdots, \alpha_r$ would be relatively prime and have only units as their common divisor.

In particular, if α_1 and α_2 are relatively prime, the above relation becomes

$$\alpha_1\gamma_1+\alpha_2\gamma_2=1.$$

EXAMPLES

1. If α_1, α_2 and β are algebraic integers, α_1 and β being relatively prime, and if $\alpha_1\alpha_2$ is divisible by β, then is α_2 divisible by β.

2. If α_1 is relatively prime to β as is also α_2, then is $\alpha_1\alpha_2$ relatively prime to β.

3. If an integer γ is divisible by two integers α and β that are relatively prime, then is γ divisible by $\alpha\beta$.

Observe, however, as has been indicated in Vol. I, Art. 112, that we get into difficulties as soon as the discussion is not limited to a fixed realm.

ART. 86. In this connection,[1] but to make a digression from the work of Hurwitz, let $\mathfrak{p}$ be a prime ideal that is not a principal ideal, and put

$$\mathfrak{p}^h = \pi\mathfrak{o},$$

where $\mathfrak{p}$ and the integer π belong to the same realm, $\Re(\alpha)$, say. If we put $\pi^{\frac{1}{h}} = \beta$ and if τ is any integer of $\mathfrak{p}$, then is τ^h divisible by $\mathfrak{p}^h$ and therefore also by $\pi = \beta^h$. It follows that τ is divisible by β. And further if τ is any integer of the fixed realm, which is divisible by β, then is τ^h divisible by β^h, and that is, by π. It follows that τ^h is a number contained in the ideal $\mathfrak{o}\pi = \mathfrak{p}^h$ and that $\mathfrak{o}\tau$ is divisible by $\mathfrak{p}$. Accordingly, the ideal $\mathfrak{p}$ may be looked upon as the collectivity of the integers of the fixed realm which are divisible by β. If we call the algebraic integer β, an *ideal* number of $\Re(\alpha)$, which has a real existence in some realm in general other than the realm $\Re(\alpha)$, then, corresponding to every prime ideal $\mathfrak{p}$ there may be associated an ideal integer β; and those integers that belong to $\Re(\alpha)$ and are multiples of β constitute the complex of numbers $\mathfrak{p}$. From this point of view the factorization of the principal ideal $\mathfrak{o}\gamma$, or of the integer γ into its prime ideal factors according to the formula

$$\mathfrak{o}\gamma = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\cdots\mathfrak{p}_r^{a_r}$$

has its complete analogue in the formula

$$\gamma = \beta_1^{a_1}\beta_2^{a_2}\cdots\beta_r^{a_r}.$$

Here the *ideality* of the numbers $\beta_1, \beta_2, \cdots, \beta_r$ means only their non-existence as algebraic integers in $\Re(\alpha)$.

[1] See also Bachmann, *Allgemeine Arithmetik der Zahlenkörper*, p. 208.

These numbers are different from the *Kummer*[1] *Numbers* (Vol. I, 272), which also have no real existence in the fixed realm, but like the atoms and electrons they have served to put into existence a very potent branch of science. (See also Arts. 55, 56 and 57.)

ART. **87.** The theorem that *every ideal may be expressed as the greatest common divisor of two principal ideals* was proved by Hurwitz as follows:

Consider first the ideal

$$\mathfrak{d} = (\alpha, \beta, \gamma).$$

It may be proved that there is an integer λ *of the fixed realm, such that*

$$\mathfrak{d} = (\alpha, \beta + \lambda\gamma).$$

In the proof it is assumed that none of the integers α, β, γ is zero. Since α, for example, being an element of $\mathfrak{d}$ is divisible by $\mathfrak{d}$, we may write

$$\mathfrak{o}\alpha = \mathfrak{d}\mathfrak{a} \tag{1}$$

and similarly $\mathfrak{o}\beta = \mathfrak{d}\mathfrak{b}$, $\mathfrak{o}\gamma = \mathfrak{d}\mathfrak{c}$. And as $\mathfrak{d}$ is equal to $\mathfrak{o}\alpha + \mathfrak{o}\beta + \mathfrak{o}\gamma$, it is seen that the greatest common divisor expressed through

$$\mathfrak{a} + \mathfrak{b} + \mathfrak{c} \tag{2}$$

is equal to $\mathfrak{o}$. As a special case, for example, if $\mathfrak{a} = \mathfrak{o}$, it would follow from (1) that both $\mathfrak{o}\beta$ and $\mathfrak{o}\gamma$ are divisible by α, and we would have at once

$$\mathfrak{d} = (\alpha, \beta, \gamma) = (\alpha) = (\alpha, \beta).$$

In this case the theorem is proved by putting $\lambda = 0$.

If, however, $\mathfrak{a}$ is different from $\mathfrak{o}$, it may be factored into its prime ideal factors in the form

$$\mathfrak{a} = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2} \cdots \mathfrak{p}_r^{a_r}.$$

Let $\mathfrak{p}_i^{d_i}$ be the highest power of $\mathfrak{p}_i$ which is a factor of $\mathfrak{d}$, so that $d_i = 0$, if $\mathfrak{p}_i$ is relatively prime to $\mathfrak{d}$. Finally, let

[1] See Kummer, *Crelle*, Vol. 35, p. 325.

λ_i be 0 or 1, according as the ideal $\mathfrak{o}\beta$, which from (1) is divisible $\mathfrak{p}_i^{d_i}$ is *not* divisible by or *is* divisible by $\mathfrak{p}_i^{d_i+1}$. It is then clear that if $\lambda_i = 1$, the ideal $\gamma\mathfrak{o}$ which from (1) is also divisible by $\mathfrak{p}_i^{d_i}$, cannot be divisible by $\mathfrak{p}_i^{d_i+1}$; otherwise even when $d_i = 0$, the three ideals $\mathfrak{a}$, $\mathfrak{b}$ and $\mathfrak{c}$ would have the common factor $\mathfrak{p}_i$, contrary to the assumption indicated in (2). Accordingly, for each of the indices $i = 1, 2, \cdots, r$, the congruence

$$\beta + \lambda_i\gamma \equiv 0$$

exists (mod. $\mathfrak{p}_i^{d_i}$), but *not* (mod. $\mathfrak{p}_i^{d_i+1}$).

If then we determine an integer λ (Vol. I, Art. 143), which satisfies the congruences

$$\lambda \equiv \lambda_1 \text{ (mod. } \mathfrak{p}_1^{d_1+1}\text{)}, \lambda \equiv \lambda_2 \text{ (mod. } \mathfrak{p}_2^{d_2+1}\text{)}, \cdots, \lambda = \lambda_r \text{ (mod. } \mathfrak{p}^{d_r+1}\text{)},$$

it is seen that the integer $\beta + \lambda\gamma$ is divisible by every prime ideal which divides $\mathfrak{d}$, namely, $\mathfrak{p}_i$ raised to the power d_i, but to no higher power.

Accordingly, if we write

$$\mathfrak{o}(\beta + \lambda\gamma) = \mathfrak{d}\mathfrak{n},$$

the ideal $\mathfrak{n}$ is relatively prime to $\mathfrak{a}$, so that

$$\mathfrak{a} + \mathfrak{n} = \mathfrak{o}.$$

It then follows from equations (1) and (2) that

$$\mathfrak{d} = \mathfrak{o}\alpha + \mathfrak{o}\beta + \mathfrak{o}\gamma = \mathfrak{o}\alpha + \mathfrak{o}(\beta + \lambda\gamma) \qquad \text{or} \qquad \mathfrak{d} = (\alpha, \beta + \lambda\gamma).$$

A repeated application of the lemma shows that every ideal

$$\mathfrak{i} = (\alpha, \alpha_1, \alpha_2, \cdots, \alpha_r)$$

may be reduced to the form of an ideal of two elements

$$\mathfrak{i} = (\alpha, \omega).$$

ART. 88. The question when are two ideals (α, ω) and (α', ω') equal, is answered by Hurwitz [1] through the following theorem:

[1] Hurwitz, "Die immodularen Substitutionen in einem algebraischen Zahlenkörper," *Göttingen Nachrichten*, 1895, p. 332.

THEOREM. *In order that two ideals* (α, ω) *and* (α', ω') *be equal, it is necessary and sufficient that the two pairs of numbers* $\alpha, \omega; \alpha', \omega'$, *be equivalent to each other, and that is, that*

$$\alpha' = \lambda\alpha + \mu\omega, \qquad \omega' = \nu\alpha + \rho\omega, \tag{1}$$

where the integers λ, μ, ν, ρ *of the fixed realm, to which the given pairs of integers also belong, satisfy the condition*

$$\lambda\rho - \mu\nu = 1. \tag{2}$$

For, if the equations (1) and (2) exist, it follows that

$$\alpha = \rho\alpha' - \mu\omega', \qquad \omega = -\nu\alpha' + \lambda\omega',$$

and every number of the ideal (α', ω') belongs to (α, ω) and vice versa.

On the other hand, if the two ideals are equal, and that is if

$$\mathfrak{i} = (\alpha, \omega) = (\alpha', \omega');$$

and, if we write

$$\mathfrak{i}^h = \mathfrak{o}\gamma, \qquad \gamma_0 = \gamma^{\frac{1}{h}},$$

it follows that

$$\gamma = \gamma_0^h = \alpha\xi + \omega\eta, \qquad \gamma_0^h = \alpha'\xi' + \omega'\eta' = \gamma,$$

where $\alpha, \omega, \alpha', \omega'$ are divisible by γ_0, while ξ, η, ξ', η' are integers of the realm and are divisible by γ_0^{h-1}.

If we define λ, μ, ν, ρ, through the relations

$$\lambda = \frac{\alpha'\xi + \omega\eta'}{\gamma}, \quad \mu = \frac{\alpha'\eta - \alpha\eta'}{\gamma}, \quad \nu = \frac{\omega'\xi - \omega\xi'}{\gamma}, \quad \rho = \frac{\omega'\eta + \alpha\xi'}{\gamma},$$

it is seen that they are integers of the realm that satisfy the equations (1) and (2). For, writing $-\gamma$ in the two forms

$$-\gamma = \begin{vmatrix} \xi, & \omega \\ \eta, & -\alpha \end{vmatrix} \quad \text{and} \quad -\gamma = \begin{vmatrix} \alpha', & \eta' \\ \omega', & -\xi' \end{vmatrix},$$

it is seen that

$$\gamma^2 = \begin{vmatrix} \xi\alpha' + \omega\eta', & \xi\omega' - \omega\xi' \\ \eta\alpha' - \alpha\eta', & \eta\omega' + \alpha\xi' \end{vmatrix} = \begin{vmatrix} \lambda\gamma, & \nu\gamma \\ \mu\gamma, & \rho\gamma \end{vmatrix},$$

or

$$1 = \lambda\rho - \mu\nu.$$

Accordingly, the integers α', ω' are equivalent to α, ω. The number $\zeta = \frac{\alpha}{\omega}$ is said to be the number of the realm *associated* with the ideal (α, ω).

Since every number ζ of a realm may be expressed in an infinite number of ways as the quotient of two integers of the realm and as every such expression of ζ is associated with an ideal, it is seen that *every number of the realm is associated with a whole class of equivalent ideals; and inversely, all numbers that are associated with the ideals of one and the same class are equivalent in the sense defined below.*

Let any number $\zeta = \frac{\alpha'}{\omega'}$ of the fixed realm be associated with the ideal (α', ω'). If (α, ω) is a second ideal that is equivalent to the first, we have

$$\gamma(\alpha', \omega') = \gamma'(\alpha, \omega), \tag{3}$$

where γ and γ' are integers of the realm.

From the preceding theorem it follows that

$$\gamma\alpha' = \lambda\alpha\gamma' + \mu\omega\gamma', \qquad \gamma\omega' = \nu\alpha\gamma' + \rho\omega\gamma', \tag{4}$$

where

$$\lambda\rho - \mu\nu = 1.$$

Through division it is seen that

$$\zeta = \frac{\alpha'}{\omega'} = \frac{\lambda\alpha + \mu\omega}{\nu\alpha + \rho\omega},$$

so that ζ is associated with the ideal $(\lambda\alpha + \mu\omega, \nu\alpha + \rho\omega)$, which from a preceding theorem is equal to (α, ω).

If on the other hand $\zeta = \frac{\alpha}{\omega}$, $\zeta' = \frac{\alpha'}{\omega'}$ are two numbers of the realm which are associated with ideals that belong to the same class, then the ideals (α, ω) and (α', ω') must

satisfy the equation (3), from which are derived (4). From the latter, through division, we have

$$\zeta' = \frac{\lambda\zeta + \mu}{\nu\zeta + \rho}, \qquad \lambda\rho - \mu\nu = 1,$$

a relation which may be used to define two *equivalent numbers* ζ *and* ζ'. See also Dedekind's *Werke*, Vol. I, pp. 174 ff. It seems that the theory as outlined in the preceding articles may be made fundamental in the theories of the Multiplication of Elliptic Function, of the Elliptic Modular Functions, etc. Note the historical sketch in Klein's *Gesammelten mathematischen Abhandlungen*, Vol. III, pp. 3–9.

CHAPTER VI

THE DIVISORS OF THE DISCRIMINANT

I. The Irregular Divisors. Hensel's Work

Art. **89.** Let α satisfy an irreducible equation of the nth degree, and form the realm $\Omega = \Re(\alpha)$. Let $\mathfrak{o}$ be the order-modul of this realm consisting of all the integers in Ω; and let $\omega_1, \omega_2, \cdots, \omega_n$ be a basis of all integers of $\mathfrak{o}$. Then $\Delta(\omega_1, \omega_2, \cdots, \omega_n) = \Delta(\mathfrak{o}) = D$, is the discriminant [fundamental invariant of $\Re(\alpha)$; see Art. 76; Vol. I, Art. 94].

If $\gamma_1, \gamma_2, \cdots, \gamma_n$ are any integers of $\mathfrak{o}$, it was seen (Vol. I, Art. 94) that

$$\gamma_i = c_{1i}\omega_1 + c_{2i}\omega_2 + \cdots + c_{ni}\omega_n \quad (i = 1, 2, \cdots, n),$$

where the c's are rational integers.

We also saw that

$$\Delta(\gamma_1, \gamma_2, \cdots, \gamma_n) = |c_{ik}|^2 D;$$

and that (Vol. I, Art. 94) the γ's form a basis of the realm, if $|c_{ik}| \neq 0$.

In particular, if $\gamma_1 = 1, \gamma_2 = \gamma, \gamma^3 = \gamma^2, \cdots, \gamma_n = \gamma^{n-1}$, then (Vol. I, Art. 63)

$$\Delta(1, \gamma, \gamma^2, \cdots, \gamma^{n-1}) = C^2 D, \tag{1}$$

where C is constant. The rational integer C is called (Vol. I, Art. 94) the *index* of the integer γ. If $C \neq 0$, the integer γ is a number that generates the realm $\Re(\alpha)$ and (Vol. I, Art. 61) is an integer of the Gattung $G(\alpha) = \mathfrak{G}$.

Corresponding to every integer γ of $\mathfrak{G}$ there is a rational integer C; and from above, the square of this integer multiplied by D is the discriminant of γ.

Every prime factor p of D is accordingly a factor of the discriminant of every integer γ of $\mathfrak{G}$.

In particular instances, examples of which are found in Arts. 99 and 100, it may happen that the discriminant of every integer γ of $\mathfrak{G}$ may have as a factor a rational prime integer p which divides the index C of γ; and that is, in the formula (1), which may be written

$$\Delta(\gamma) = C^2(\gamma) D,$$

there exists a prime rational integer p which divides the index $C(\gamma)$, where γ goes through all the integers of $\mathfrak{G}$.

The divisors of $C = C(\gamma)$ Kronecker [1] called *unessential* (*Ausserwesentliche*). These divisors (*op. cit.*, p. 69) he also called *irregular*, the regular or essential divisors being those of the fundamental invariant D. The latter nomenclature is adopted in the present treatise.

ART. 90. Write

$$(1) \qquad \gamma^i = c_{1i}\omega_1 + c_{2i}\omega_2 + \cdots + c_{ni}\omega_n \quad (i = 0, 1, 2, \cdots, n-1),$$

and observe that, if p is a factor of the determinant

$$C = \begin{vmatrix} c_{10}, & \cdots, & c_{n0} \\ \cdot & \cdot & \cdot \\ c_{1,\,n-1}, & \cdots, & c_{n,\,n-1} \end{vmatrix},$$

rational integers $g_1, g_2, \cdots, g_n$ may be found (Vol. I, Art. 56), such that

$$(2) \quad c_{i1}g_1 + c_{i2}g_2 + \cdots + c_{in}g_n \equiv 0 \pmod{p} \quad (i = 0, 1, 2, \cdots, n-1).$$

From this it follows that

$$(3) \qquad g_1 + g_2\gamma + \cdots + g_n\gamma^{n-1} \equiv 0 \pmod{p};$$

and therefrom it is seen that γ satisfies (mod. p) a congruence of degree less than n, the degree of the realm Ω. Hence if there is a divisor p of the index $C(\gamma)$ of every integer γ of the Gattung $\mathfrak{G}$ of Ω, it follows that every integer that creates the realm Ω of the nth degree,

[1] Kronecker, *Monatsbericht der Berliner Akademie*, March 1879, p. 214; *Grundzüge*, p. 23, footnote.

when considered (mod. p), satisfies a congruence of degree less than n.

If p is not an irregular divisor, and that is, one that does not divide $C(\gamma)$, then γ (mod. p) *cannot* satisfy a congruence of degree less than n. For, by substituting the values (1) in (3) there would necessarily result a system of equations (2) with a determinant C which is divisible by p, contrary to the assumption.

We may accordingly say: *Then and only then is the integral congruence (mod. p) with rational integral coefficients, which the integer γ of $\mathfrak{G}$ satisfies, of degree less than n, if p is an irregular divisor of the discriminant $\Delta(\gamma)$; and that is, if*

$$C(\gamma) \equiv 0 \pmod{p}.$$

It is thus seen that the question *whether or not a prime integer p is a divisor of the index $C(\gamma)$ of every integer γ of $\mathfrak{G}$* reduces to the question *whether or not (mod. p) the congruence that every integer γ of $\mathfrak{G}$ satisfies, is of degree less than n.*

ART. **91.** If $F(x) = 0$ is the irreducible equation which γ satisfies and if p is a prime integer that does *not* divide $C(\gamma)$, Dedekind [1] was able to prove that corresponding to a factorization of $F(x)$ into its irreducible factors (mod. p), say

$$F(x) \equiv P_1(x)^{a_1} P_2(x)^{a_2} \cdots P_r(x)^{a_r} \pmod{p},$$

there exists a corresponding factorization of p into its ideal prime factors

$$p = \mathfrak{p}_1^{a_1} \mathfrak{p}_2^{a_2} \cdots \mathfrak{p}_r^{a_r} \qquad \text{(see Arts. 74, 75).}$$

This conformity, necessary for the establishment of the fundamental law relative to the unique factorization of algebraic numbers, was seen to fail, however, when p was

[1] Dedekind, "Ueber den Zusammenhang zwischen der Theorie der Idealen und der Theorie der höheren Kongruenzen," *Göttingen Abh.*, Vol. 23, 1878; and *Göttingen Anz.*, 1871, p. 1488. See also Kronecker, *Grundzüge*, § 25.

an irregular divisor of the discriminant of $\Delta(\gamma)$, that is, when p was a divisor of $C(\gamma)$. With this discovery was also seen the reason for the failure of Kummer's conjecture, which had to do with the establishment of a general theory of ideal numbers, founded upon the congruence $F(x) \equiv 0 \pmod{p}$, a theory which was sufficient for the case of the cyclotomic realms, namely, those realms which were formed of the roots of unity.

If p divides the index of every integer γ of $\mathfrak{G}$, it is impossible to use an equation of the nth degree

$$F(x) = 0,$$

which γ satisfies, in order that, through the factorization of $F(x)$ into its irreducible factors (mod. p), we may proceed to a factorization of p into its prime ideal factors by means of the Theory of Higher Congruences. And so the establishment of the theory in question in such a realm, namely, where p divides the index of every γ that creates the realm, is not permissible, the result being that the general theory is faulty. This trouble was experienced by Kronecker. (See, for example, § 25 of the *Grundzüge*.) We are therefore emphasizing Hensel's work in the presentation of this chapter, as well as the fact that Dedekind also used the method of higher congruences.

ART. 92. To make a resumé of what has been proved previously (Art. 74) and at the same time to set the proposal of this chapter in definite form, with Hensel[1] let the left hand side of the fundamental equation be factored into its irreducible (mod. p) divisors, namely,

$$F(x) \equiv P_1(x)^{a_1} P_2(x)^{a_2} \cdots P_h(x)^{a_h} \pmod{p},$$

and observe that the derivative of this expression is

$$F'(x) = P_1(x)^{a_1-1} P_2(x)^{a_2-1} \cdots P_h(x)^{a_h-1} \Phi(x) + p\Psi(x),$$

[1] Hensel, *Crelle's Journal*, Vol. 113, pp. 79 et seq.

where

$$\Phi(x) = a_1 P_2(x) \cdots P_h(x) + a_2 P_1(x) P_3(x) \cdots P_h(x) + \cdots,$$

and where $\Psi(x)$ is an integral function of x with rational integral coefficients. Further, observe that $\Phi(x)$, considered mod. p, is relatively prime to each of the prime functions $P_i(x)$, provided that none of the coefficients a_i is divisible by p.

If we write for x the fundamental form

$$\xi = u_1\omega_1 + u_2\omega_2 + \cdots + u_n\omega_n,$$

it is seen that $F'(\xi)$ is divisible by $\mathfrak{p}_1^{a_1-1}\mathfrak{p}_2^{a_2-1}\cdots\mathfrak{p}_h^{a_h-1}$, and we may accordingly write

$$F'(\xi) = (\xi-\xi_1)(\xi-\xi_2)\cdots(\xi-\xi_{n-1}) = \mathfrak{p}_1^{a_1-1}\mathfrak{p}_2^{a_2-1}\cdots\mathfrak{p}_h^{a_h-1}H(\xi),$$

where the function $H(\xi)$ is *not* divisible by p. Taking the norm of this expression, we have (Art. 76 and Vol. I, Art. 96)

$$N(F'(\xi)) = \Pi(\xi-\xi_k) = \Delta(1, \xi, \cdots, \xi^{n-1}) = \Delta(\xi) = D\,|\,U_{gh}\,|^2.$$

Since

$$N(\mathfrak{p}_i) = p^{f_i},$$

it is seen that

$$\Delta(\xi) = p^{f_1(a_1-1)+f_2(a_2-1)+\cdots+f_h(a_h-1)}L(u_1, u_2, \cdots, u_n),$$

where L is an integral function in u_i with rational integral coefficients that are not all divisible by p.

If the degree of the product $\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_h$ *is denoted by* r, *and that is, if* $N(\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_h) = p^r$, *and if we observe that* $a_1f_1 + a_2f_2 + \cdots + a_hf_h = n$, *it is seen that the discriminant of the fundamental equation, and that is, the discriminant of the Gattung* $\mathfrak{G}$, *and that is,* $\Delta(\xi)$ *is divisible by* p *to the power* $n-r$ *and no higher.*

The exceptional case, where one of the exponents a_i is divisible by p, will be considered in Chapter XVI. The preceding deduction shows in this exceptional case also that the $(n-r)$th power of p is a factor of $\Delta(\xi)$,

although not the highest power of p that divides this discriminant; for in that case $\Phi(\xi)$ is divisible by one of the functions $P(\xi)$.

The following is a corollary of this general theorem: *A rational prime integer p is then and only then a factor of the discriminant of a Gattung, if within this Gattung, p contains one or several prime ideal factors to the second or higher powers* (Art. 31).

For the integer $n-r$ is then and only then different from zero, if at least one of the exponents a_i is greater than unity. And it follows at once, since the discriminant can have only a finite number of prime factors p, that there are only a finite number of such primes which admit prime ideal factors to powers higher than the first. This is Dedekind's [1] *fundamental theorem* by means of which he wished to establish a general theory of algebraic integers. Instead of the fundamental form ξ which was introduced above and which includes impartially all algebraic integers of a fixed realm, he employed a special algebraic integer

$$\gamma = g_1\omega_1 + g_2\omega_2 + \cdots + g_n\omega_n.$$

To the rational integers $g_1, g_2, \cdots, g_n$ he gave such values that γ would satisfy a congruence (mod. p) of degree n, the degree of the realm. This he was able to do when and only when the determinant above $|U_{gh}|$ is *not* divisible by p for all systems of rational integral values $u_1 = g_1,\ u_2 = g_2,\ \cdots,\ u_n = g_n$. It is proved in the sequel that such cases exist, where $|U_{gh}|$ is divisible by p for all such systems of values and definite examples are given of realms in which this is true. And thus, the general theory as given in Dedekind's plan, where the investigation has to do only with the algebraic integers themselves

[1] Dedekind, "Ueber die Discriminanten endlicher Körper," *Göttingen Abh.*, Vol. 29.

and not with the fundamental form, must in a measure be replaced by a theory that is based upon the consideration of the algebraic forms which lead more simply and more directly to the desired end. (See preceding article, end.)

ART. 93. It was seen (Art. 76) that the discriminant [1] of the fundamental form

$$\xi = u_1\omega_1 + u_2\omega_2 + \cdots + u_n\omega_n$$

was

$$\Delta(\xi) = |U_{gh}|^2 D.$$

To put in evidence the indeterminates u_i, write

$$|U_{gh}| = \theta(u_1, u_2, \cdots, u_n).$$

It was seen in Art. 76 that $\theta(u_1, u_2, \cdots, u_n)$ is a *unit* form; and that is, it is *not* divisible by any prime integer p; and that is, the discriminant of the fundamental form does *not* have irregular (*ausserwesentlich*) divisors.

Observe, however, that this discriminant becomes $\Delta(\gamma) = \theta(g_1, \cdots, g_n)^2 D$, if instead of ξ is written the algebraic integer

$$\gamma = g_1\omega_1 + g_2\omega_2 + \cdots + g_n\omega_n.$$

And it is also seen that the rational integer $\theta(g_1, g_2, \cdots, g_n)$ is the index $|c_{ik}|$ of Art. 89.

The prime integers p which are the divisors of $\theta(g_1, g_2, \cdots, g_n)$ are the irregular divisors of the discriminant of γ, and that is, of $C(\gamma)$. The question whether for every γ of the Gattung $\mathfrak{G}$ there is the same prime factor p of $C(\gamma)$ is settled, if it is shown that $\theta(u_1, u_2, \cdots, u_n)$ is divisible by p for every system of integral values that may be assigned to the indeterminates $u_1, u_2, \cdots, u_n$.

This question is answered in the theorem of Vol. I, Art. 202, namely: In order that a prime integer p be a

[1] See Hensel, *Theorie der algebraischen Zahlen*, Chapt. XII.

common divisor (irregular) of the discriminant of all integers γ of $\mathfrak{G}$, it is necessary and sufficient that the function $\theta(u_1, u_2, \cdots, u_n)$ be contained in the modular system

$$(p, u_1^p - u_1, u_2^p - u_2, \cdots, u_n^p - u_n);$$

and that is, that $\theta(u_1, u_2, \cdots, u_n)$ be of the form

$$pU + (u_1^p - u_1)U_1 + \cdots + (u_n^p - u_n)U_n,$$

where $U, U_1, \cdots, U_n$ are integral functions in $u_1, u_2, \cdots, u_n$ with rational integral coefficients. When the coefficients have been reduced, modulo p, and due to the Fermat Theorem, the exponents of the several u's have been reduced, modulo $p-1$, the resulting form must be identically zero. When this is true, p is an irregular divisor of the discriminant of every integer γ of $\mathfrak{G}$. (See Examples in Arts. 99 and 100.)

ART. **94.** An important consequence was derived in Art. 75, namely, the fundamental form ξ satisfies no congruence (mod. p) of less degree than the degree n of the fixed realm. And this was true for all integers p. Instead of the fundamental form ξ take any algebraic integer of the Gattung and investigate the congruence which it satisfies (mod. p). It is clear that, if $F(x) = 0$ is the fundamental equation which is satisfied by ξ, then

$$F(x) \equiv P_1(x)^{a_1} P_2(x)^{a_2} \cdots P_h(x)^{a_h} \equiv 0 \pmod{p}$$

is satisfied for γ, when for $x = \xi = u_1\omega_1 + u_2\omega_2 + \cdots + u_n\omega_n$, we write $u_1 = g_1, u_2 = g_2, \cdots, u_n = g_n$.

The question arises what are the necessary conditions to be fulfilled, in order that γ satisfy no congruence (modulo p) of less degree than n, and that is, determine the necessary conditions that p shall *not* divide $C(\gamma)$.

Let

$$u_i = g_i \qquad (i = 1, 2, \cdots, n),$$

be substituted in the functions $P(x)$ above, after ξ has

been written for x, and let them be denoted by $Q(x)$. The above congruence is satisfied by γ and becomes

$$Q_1(x)^{a_1}Q_2(x)^{a_2}\cdots Q_h(x)^{a_h}\equiv 0 \pmod{\mathfrak{p}}.$$

It will be shown [1] *first* that the functions $Q(x)$ must be irreducible, mod. p. For, if, say $Q_1(x)\equiv E_1(x)G_1(x)$ (mod. p), then also this congruence exists (mod. $\mathfrak{p}_1$); and since $P_1(x)\equiv 0$ (mod. $\mathfrak{p}_1$) is satisfied for $x=\xi$, it is also satisfied when rational integers are written for the indeterminates u_i; and that is,

$$E_1(\gamma)G_1(\gamma)\equiv 0 \pmod{\mathfrak{p}_1}.$$

With this it would follow (Art. 26) that either $E_1(\gamma)$ or $G_1(\gamma)\equiv 0$ (mod. $\mathfrak{p}_1$), say $E_1(\gamma)\equiv 0$ (mod. $\mathfrak{p}_1$).

It would follow further that

$$E_1(\gamma)^{a_1}P_2(\gamma)^{a_2}\cdots P_h(\gamma)^{a_h}\equiv 0 \pmod{p};$$

and that is, γ satisfies a congruence (mod. p) of degree less than n, since the degree of $E_1(x)$ is less than that of $P_1(x)$.

It will be shown *secondly* that the functions $Q_1(x)$, $Q_2(x)$, $\cdots$, $Q_r(x)$ must be all different (mod. p). For, were $Q_1(x)\equiv Q_2(x)$ (mod. p), it would follow that

$$Q_1(\gamma)\equiv 0\equiv Q_2(\gamma) \pmod{\mathfrak{p}_1}$$

and

$$Q_2(\gamma)\equiv 0\equiv Q_1(\gamma) \pmod{\mathfrak{p}_2}.$$

If then, $a_1\geqq a_2$, it would also follow that $Q_1(\gamma)^{a_1}$ is divisible by both $\mathfrak{p}^{a_1}$ and by $\mathfrak{p}^{a_2}$ and accordingly γ would be a root of

$$Q_1(x)^{a_1}\cdot Q_3(x)^{a_3}\cdots Q_h(x)^{a_h}\equiv 0 \pmod{p},$$

a congruence, whose degree is less than n.

With this it is seen that *for the existence of an integer γ of the Gattung $\mathfrak{G}$, whose index $C(\gamma)$ is not divisible by the prime integer*

$$p=\mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\cdots\mathfrak{p}_h^{a_h},$$

[1] Hensel, *Crelle*, Vol. 113, p. 130. It is well to study this paper of Hensel in juxtaposition with the one of Dedekind mentioned above.

there must exist h incongruent prime functions (mod. p), whose degrees $f_1, f_2, \cdots, f_h$ *are the degrees of the prime ideals* $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_h$.

The above conditions are also sufficient [1] for the existence of such a number γ. To prove this, corresponding to every prime ideal factor $\mathfrak{p}_i$ of p choose a prime function P_i of degree f_i, which is also the degree of $\mathfrak{p}_i$ (Art. 61). Let ρ_i be such a root of the congruence

$$P_i(x) \equiv 0 \pmod{\mathfrak{p}_i}$$

that

$$\mathfrak{p}_i = (p, P_i(\rho_i)),$$

where $P_i(\rho_i)$ is divisible by $\mathfrak{p}_i$, but not by $\mathfrak{p}_i^2$. Proceed in a similar way for all the functions $P_i(x)$ $(i=1, 2, \cdots, h)$.

Further (Art. 33) determine an integer ρ which satisfies the h congruences

$$\rho \equiv \rho_i \pmod{\mathfrak{p}_i} \qquad (i=1, 2, \cdots, h).$$

We are thus able to form h congruences

$$P_i(\rho) \equiv P_i(\rho_i) \pmod{\mathfrak{p}_i^2},$$

in which the integer $P_i(\rho)$ is divisible by $\mathfrak{p}_i$ to the first but no higher power.

Observe next (Art. 61) that a congruence

$$\varphi(\rho) \equiv 0 \pmod{\mathfrak{p}_i^{a_i}},$$

whose coefficients are rational integers that are not all divisible by p, has the same meaning as the congruence

$$\varphi(x) \equiv 0 \pmod{p, P_i(x)^{a_i}}.$$

It follows, if $p = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\cdots\mathfrak{p}_h^{a_h}$, that the congruence

$$\varphi(\rho) \equiv 0 \pmod{\mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\cdots\mathfrak{p}_h^{a_h}}$$

has the same significance as

$$\varphi(x) \equiv 0 \pmod{p, R(x)}, \tag{1}$$

where $R(x) = P_1(x)^{a_1}P_2(x)^{a_2}\cdots P_h(x)^{a_h}$. For, observe

[1] See Bachmann, *Allgemeine Arithmetik*, etc., p. 273.

that the product of any two modular systems is

$$(2)\quad (p, P_1(x)^{a_1})(p, P_2(x)^{a_2}) = (p^2, pP_1(x)^{a_1}, pP_2(x)^{a_2}, P_1(x)^{a_1}P_2(x)^{a_2}).$$

Further, since $P_1(x)^{a_1}$ and $P_2(x)^{a_2}$, under the given assumptions are different and relatively prime, we may find two functions $\Phi(x)$ and $\Psi(x)$ such that

$$P_1(x)^{a_1}\Phi(x)+P_2(x)^{a_2}\Psi(x)\equiv 1 \pmod{p}.$$

From this it is seen that p may be added as an element to the right hand side of (2), which then reduces to

$$(p, P_1(x)^{a_1}P_2(x)^{a_2}).$$

And this process continued produces (1).

Writing (1) in the form

$$\varphi(x)\equiv R(x)\cdot S(x) \pmod{p},$$

where $S(x)$ is an integral function with rational integral coefficients, it is seen, since $R(x)$ is of degree n, that the degree of the function $\varphi(x)$ which ρ satisfies (mod. p) must be at least n. Observe further that n is the degree of the congruence

$$P_1(x)^{a_1}\cdots P_h(x)^{a_h}\equiv 0 \pmod{p},$$

which ρ satisfies.

ART. **95.** It is usually the case that the fundamental invariant D, the discriminant of the fixed realm, has not been determined; and it often involves considerable work in deriving it. Consequently it is desirable to have a method of finding the prime factors of the index of an integer without first determining its discriminant. This may be done by the following *Dedekind Method* (" Theorie der Ideale, etc.," *Gött. Abh.*, Vol. 23):

Let γ be any integer of the Gattung of the fixed realm, and let $F(x)=0$ be the irreducible equation of the nth degree which γ satisfies. Let $F(x)$ be factored (mod. p) into its

irreducible factors, taking the form

$$F(x) = \Pi(x) - pM(x), \tag{1}$$

$\Pi(x)$ *denoting the product of the irreducible factors, and* $M(x)$ *an integral function of* x *with rational integral coefficients. The necessary and sufficient condition that* p *be a factor of the index of* γ *consists in that there be a multiple prime factor* $P(x)$ *of* $\Pi(x)$, *which is also a factor of* $M(x)$ *(mod.* p*).*

To prove this, first let p be a prime integer that is *not* a factor of the index of γ and let the prime ideal factor of p in the fixed realm be

$$p = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\cdots\mathfrak{p}_h^{a_h},$$

so that

$$F(\gamma) \equiv P_1(\gamma)^{a_1}P_2(\gamma)^{a_2}\cdots P_h(\gamma)^{a_h} \pmod{p},$$

where $P_i(\gamma)$ is divisible by $\mathfrak{p}_i$ to the first power only, but by none of the other ideal factors of p.

If D is divisible by p, one of the integers a_i is greater than unity. It is seen that here also $P_i(\gamma)$ cannot be divisible by $\mathfrak{p}_i^2$. For, were $P_1(\gamma)$, for example, divisible by $\mathfrak{p}_1^2$ and $a_1 > 1$, it would follow that

$$P_1(\gamma)^{a_1-1}P_2(\gamma)^{a_2}\cdots P_h(\gamma)^{a_h}$$

was divisible by p and accordingly γ would be the root of a congruence

$$P_1(x)^{a_1-1}P_2(x)^{a_2}\cdots P_h(x)^{a_h} \equiv 0 \pmod{p}$$

of degree less than n, which is not true (Art. 94).

And further, were $P_1(\gamma)$ divisible by, say $\mathfrak{p}_2$, the two congruences $P_1(x) \equiv 0$, $P_2(x) \equiv 0 \pmod{p}$ would have a common root. This is *not* true, for since $P_1(x)$ and $P_2(x)$ are prime functions (mod. p), there exists a congruence of the form

$$P_1(x)\Phi_1(x) + P_2(x)\Phi_2(x) \equiv 1 \pmod{p}.$$

And, writing $x=\gamma$ in this congruence, it would follow that

$$0\equiv 1 \pmod{\mathfrak{p}_2}.$$

Writing $x=\gamma$ in (1), we have the equation

$$\Pi(\gamma)-pM(\gamma)=0,$$

and it is clear that $M(\gamma)$ is divisible by none of the ideal factors of p, since the ideal factors of p and $\Pi(\gamma)$ mutually cancel one another for all cases where p does not divide the index of γ. It follows that $M(x)$ is divisible by none of the prime functions $P_i(x) \pmod{p}$. For, were

$$M(x)=P_i(x)\Phi_i(x)+p\varphi(x),$$

it would follow for $x=\gamma$, that $M(\gamma)$ is divisible by $\mathfrak{p}$.

From this we may conclude *firstly* that if $M(x)$ is divisible by one of the prime factors $P_i(x)$ which, raised to the second or higher degrees, is a factor of $\Pi(x) \pmod{p}$, that the prime rational integer p must be a divisor of the index of γ.

Inversely, if p is a divisor of the index of γ, there exist (Art. 90) n rational integers $x_1, x_2, \cdots, x_n$ all of which are not divisible by p and such that

$$\Phi(\gamma)=x_1+x_2\gamma+\cdots+x_n\gamma^{n-1}\equiv 0 \pmod{p}.$$

Accordingly, we may denote by $A(x)$ the greatest common divisor $(\text{mod. } p)$ of the two functions $F(x)$ and $\Phi(x)$. Due to equation (1), it is seen that since $A(x)$ $(\text{mod. } p)$ is a divisor of $F(x)$, it is a divisor of $\Pi(x)$; and since it is of degree less than that of $F(x)$, it follows that

$$F(x)=A(x)B(x)-pM(x), \tag{2}$$

where $B(x)$ is an integral function of x with rational integral coefficients. Since the function $A(x)$ is at least of the first degree, it certainly has one prime function $(\text{mod. } p)$ as a factor, which may be denoted by $P(x)$. Accordingly, there are two integral functions with ra-

tional integral coefficients, say $\varphi(x)$ and $f(x)$, such that

$$\Phi(x)\varphi(x)+F(x)f(x)\equiv A(x) \text{ (mod. } p).$$

From this it is seen that $A(\gamma)$ is an algebraic integer that is divisible by p, and is therefore the root of an equation of the form

$$X^s+pa_1X^{s-1}+p^2a_2X^{s-2}+\cdots+p^sa_s=0.$$

Consequently, there exists the identity

$$A(\gamma)^s+pa_1A(\gamma)^{s-1}+\cdots+p^sa_s=0,$$

where the a's are rational integers.

Multiply the above expression by $B(\gamma)^s$ and observe from (2) that

$$A(\gamma)B(\gamma)=pM(\gamma).$$

It follows that

$$M(\gamma)^s+a_1M(\gamma)^{s-1}B(\gamma)+\cdots+a_sB(\gamma)^s=0.$$

Since γ is a root of the irreducible equation $F(x)=0$, it is seen (Vol. I, Art. 41) that

$$A(x)^s+pa_1A(x)^{s-1}+\cdots+p^sa_s=F(x)Q(x),$$

and

$$M(x)^s+a_1M(x)^{s-1}B(x)+\cdots+a_sB(x)^s=F(x)R(x).$$

These equations written as congruences are

$$A(x)^s\equiv 0 \text{ (modd. } p,\ F(x)),$$

and, due to (2),

$$M(x)^s\equiv 0 \text{ (modd. } p,\ B(x)).$$

Since, modulo p, the prime function $P(x)$, which is a divisor of $B(x)$, is a divisor of $F(x)$, it follows from the first of the above congruences that $P(x)$ is a divisor, modulo p, of $M(x)$. From (2), $P(x)$ is a multiple factor modulo p, of $F(x)$. Accordingly, it follows that if p is a divisor of the index of γ, that there exists a prime function $P(x)$ which (mod. p) is a multiple factor of $\Pi(x)$ and is a factor (mod. p) of $M(x)$. With this is proved the theorem as stated. (See Dedekind, *Werke*, Vol. I, pp. 213 ff.)

ART. **96.** The results of the two preceding articles, which were discovered by Dedekind (*Götting. Abh.*, Vol. 23) suggest at once another proof for the existence of an irregular divisor of the discriminant. For the prime integer p is a factor of the index $C(\gamma)$ of every integer γ of $\mathfrak{G}$, only if there are *not* h incongruent (mod. p) prime functions $P_i(x)$ $(i=1, 2, \cdots, h)$ of degrees f_i, respectively.

In Art. 49 it was seen that the number of irreducible factors (mod. p) of degree f of the expression

$$x^{p^f}-x \qquad \text{was} \qquad \frac{1}{f}g(f),$$

where

$$g(f)=p^f-\sum_q p^{f/q}+\sum_{qq'}p^{f/qq'}-\cdots=\sum_{d/f}\mu(d)p^d,$$

and where q, q', $\cdots$ are the different prime factors of f.

The degrees of the prime ideals $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\cdots$, $\mathfrak{p}_h$, are respectively,

$$f_1, f_2, \cdots, f_h. \tag{1}$$

Some of these f's may be equal. Denote those that are unequal by f_1, f_2, $\cdots$, f_k. Denote the number of f's in the series (1) that are equal to f_1 by h_1, the number of these that are equal to f_2 by h_2, etc. It follows that

$$h_1+h_2+\cdots+h_k=h.$$

It is clear that there do not exist h incongruent (mod. p) prime functions $P_i(x)$ $(i=1, 2, \cdots, h)$, if any one of the following k inequalities exist

$$h_i>\frac{1}{f_i}g(f_i) \qquad (i=1, 2, \cdots, k). \tag{2}$$

With this is proved Hensel's Theorem:

In order that a prime integer $p=\mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\cdots\mathfrak{p}_h^{a_h}$, *where the degree of the prime ideals* $\mathfrak{p}_i$ *are respectively* f_i, *may be a common irregular divisor of the discriminants of every integer* γ *of the Gattung* $\mathfrak{G}$, *it is necessary and sufficient that at least one of the inequalities* (2) *exist.*

ART. 97. The above criterion was also derived by Hensel in another form in which a knowledge of the factorization of p within the fixed realm into its ideal factors or the distribution of the fundamental equation (mod. p) into prime factors was not assumed. For, let $\mathfrak{p}$ be any arbitrary prime factor p of degree f. Let

$$\xi = u_1\omega_1 + u_2\omega_2 + \cdots + u_n\omega_n$$

be the fundamental form of the realm and write in general (see Art. 72).

$$\xi_h = u_1\omega_1^{p^h} + \cdots + u_n\omega_n^{p^h} \qquad (h=1, 2, \cdots).$$

It is seen (Art. 72) that of the infinite number of such forms only the f forms

$$\xi, \xi_1, \cdots, \xi_{f-1}$$

for indeterminate u's are different (mod. $\mathfrak{p}$) and that

$$\xi \equiv \xi_f, \xi_1 \equiv \xi_{f+1}, \cdots, \xi_{h+f} \equiv \xi_h \cdots \text{ (mod. } \mathfrak{p}).$$

It follows at once that a linear form

$$\xi_\nu - \xi = u_1(\omega_1^{p^\nu} - \omega_1) + \cdots + u_n(\omega_n^{p^\nu} - \omega_n)$$

is divisible by the prime ideal $\mathfrak{p}$, if and only if ν is a multiple of f. If ν *is* a multiple of f, it is proved below that $\mathfrak{p}$ is a factor, but no higher power of $\mathfrak{p}$ is a factor of the above linear form. For, suppose first that $\mathfrak{p}^2$ is a factor of p and observe (Arts. 36 and 44), due to the Fermat Theorem, that

$$\xi^{p^\nu} \equiv \xi \text{ (mod. } p).$$

It would follow for every algebraic integer

$$\gamma = g_1\omega_1 + g_2\omega_2 + \cdots + g_n\omega_n$$

that

$$\gamma^{p^\nu} - \gamma \equiv 0 \text{ (mod. } \mathfrak{p}^2).$$

That this is *not* true is seen at once, if we put $\gamma = \tilde{\omega}$, where $\tilde{\omega}$ is divisible by $\mathfrak{p}$ but *not* by $\mathfrak{p}^2$. For, the above congruence reduces to

$$-\tilde{\omega} \equiv 0 \text{ (mod. } \mathfrak{p}^2),$$

which is *not* true.

If, however, $\mathfrak{p}$ occurs only to the first power in p, and if the linear form $\xi_\nu - \xi$ for indeterminate $(u_1, \cdots, u_n)$ were divisible by $\mathfrak{p}^2$, it would follow that the n elements

$$\omega_i^{p^\nu} - \omega_i \qquad (i = 1, 2, \cdots, n)$$

were each divisible by $\mathfrak{p}^2$, which in general is *not* true. For, were this true for any p and any system of basal elements $(\omega_1, \cdots, \omega_n)$, we might change one of the elements say ω_1 to $\omega_1 + p$ without changing the character (mod. p) of the basis. It would then follow that

$$(\omega_1 + p)^{p^\nu} - (\omega_1 + p) \equiv (\omega_1^{p^\nu} - \omega_1) - p \equiv -p \equiv 0 \pmod{\mathfrak{p}^2},$$

which is *not* true.

If for the element ω_1 we write $1 + p$, which (Vol. I, Art. 100) we have seen was always possible, it would follow at once that $\xi_\nu - \xi$ is *not* divisible by $\mathfrak{p}^2$.

We thus have the Theorem: *If ν is a multiple of f, the linear form $\xi_\nu - \xi = u_1(\omega_1^{p^\nu} - \omega_1) + \cdots + u_n(\omega_n^{p^\nu} - \omega_n)$ is for indeterminates $u_1, \cdots, u_n$ divisible by the first and only the first power of every prime ideal factor $\mathfrak{p}$ of p, whose degree is f.*

And it is clear that, if p contains ideal factors to the first degree only, so that

$$p \sim \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_h,$$

then we may determine a linear form $\xi_\nu - \xi$ which is divisible by p; or what is the same thing, the h congruences

$$\omega_i^{p^\nu} - \omega_i \equiv 0 \pmod{p}$$

are all satisfied. For, we have only to determine for ν the least common multiple of the h numbers $f_1, f_2, \cdots, f_h$, these being the respective degrees of $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_h$.

If, however, p contains as a factor the ideal $\mathfrak{p}$ to a power higher than the first, there is no linear form $\xi_\nu - \xi$, which is divisible by p; for none of the above differences con-

tains as a divisor any prime ideal factor of p to a power higher than the first. With this follows the theorem:

The rational prime integer p is factorable within a given realm into ideal factors, none of which is equivalent to the other, if at least one of the linear forms $\xi_\nu - \xi$ is divisible by p and only then.

The prime integer p is a divisor of the discriminant of the realm, and that is, of the fundamental invariant D, if and only if p has a prime ideal factor to at least the second power. Hence, we have as a corollary of the above theorem:

The prime integer p is then and only then a divisor of D, if one of the linear factors $\xi_\nu - \xi$ is divisible by a fractional power of p, but not by p itself.

ART. 98. Let f be an arbitrary integer and form the quotient

$$F_f(\xi) = \frac{(\xi_f - \xi)\Pi(\xi_{f/qq'} - \xi)\Pi(\xi_{f/qq'q''q'''} - \xi)\cdots}{\Pi(\xi_{f/q} - \xi)\Pi(\xi_{f/qq'q''} - \xi)\cdots},$$

where $q, q', q'', \cdots$ are the different prime factors of f.

Using the Möbius coefficient of Art. 45, this quotient may be written

$$F_f(\xi) = \prod_{d|f}(\xi_d - \xi)^{\mu(d)},$$

and is a fractional function of the $g(f)$ dimension in the basal elements

$$(\omega_1, \omega_2, \cdots, \omega_n),$$

where

$$g(f) = p^f - \sum p^{f/q} + \sum p^{f/qq'} - \cdots = \sum_{d|f}\mu(d)p^d.$$

The above quotient is equivalent to the product of all the different prime ideal divisors of p, whose degree is exactly f. For, if $\mathfrak{p}$ is a divisor of p, whose degree $\bar{f}$ is not a divisor of f, then $\mathfrak{p}$ appears in neither the numerator nor the denominator of $F_f(\xi)$. If, however, $\bar{f}$ is a divisor of f, it enters as many times in the numerator as in the

denominator of $F_f(\xi)$ and accordingly cancels out. Finally, if $\bar{f}=f$, then p enters once and only once in the numerator of $F_f(\xi)$. With this the assertion is proved.

Accordingly, if $\mathfrak{p}^{(1)}$, $\mathfrak{p}^{(2)}$, $\cdots$, $\mathfrak{p}^{(n_f)}$ are the different prime ideal factors of p, each of the fth degree, then is $F_f(\xi)$ equal to their product; and that is,

$$F_f(\xi)=\prod_{d/f}(\xi_d-\xi)^{\mu(d)}\sim\mathfrak{p}^{(1)}\mathfrak{p}^{(2)}\cdots\mathfrak{p}^{(n_f)}.$$

Taking the norm of both sides of this expression, it is seen that

$$N[F_f(\xi)]=p^{fn_f}.$$

And that is: *The form $F_f(\xi)$, which is of the $g(f)$ dimension in the basal elements, has a degree fn_f, where n_f is the number of prime ideal factors of p which are different from one another, each being of degree f. If there is no prime ideal factor of p of degree f, then naturally, $n_f=0$.*

Next write down the n forms $F_f(\xi)$, whose degrees are fn_f $(f=1, 2, \cdots, n)$. From the theorem of Art. 96 it is clear that p is then and only then an irregular divisor, and that is, a divisor of the index of the discriminant of every integer γ of the Gattung $\mathfrak{G}$, if of the inequalities

$$fn_f>g(f) \qquad (f=1, 2, \cdots, n)$$

at least one is satisfied.

Since fn_f is the degree of the form $F_f(\xi)$ and $g(f)$ its dimension in $(\omega_1, \omega_2, \cdots, \omega_n)$, this result may be expressed in the following form, which Hensel regards as " simple and elegant ":

The rational prime integer p is then and only then an irregular divisor of all discriminants $\Delta(\gamma)$ of $\mathfrak{G}$, if among the forms

$$F_f(\xi)=\prod_{d/f}(\xi_d-\xi)^{\mu(d)} \qquad (f=1, 2, \cdots, n),$$

there is at least one, whose dimension in $(\omega_1, \omega_2, \cdots, \omega_n)$ is less than its degree, and that is, less than fn_f in the

expression

$$N[F_f(\xi)]=p^{fn_f}.$$

ART. 99. The fact [1] that in reality there exist realms and Gattung such that the discriminant of every integer γ in them is divisible by a definite prime integer, is illustrated in the following two examples, the first due to Dedekind (*Göttingen Abh.*, Vol. 23, p. 30) and the second due to Hensel.

With Dedekind let $\Omega=\Re(\theta)$ be a realm determined by the root θ of the irreducible equation

$$F(x)=x^3-x^2-2x-8=0; \tag{1}$$

and let $\delta(\theta)$ be the different of θ, and that is

$$\delta(\theta)=F'(\theta)=3\theta^2-2\theta-2.$$

It follows (Vol. I, Arts. 94 and 297) that

$$\Delta(1,\ \theta,\ \theta^2)=-N[\delta(\theta)].$$

To determine this norm, observe, due to the identity

$$\theta^3-\theta^2-2\theta-8\equiv 0, \tag{2}$$

that

$$\delta(\theta)=-2-2\theta+3\theta^2,$$
$$\theta\delta(\theta)=24+4\theta+\theta^2,$$
$$\theta^2\delta(\theta)=8+26\theta+5\theta^2;$$

and accordingly

$$\begin{vmatrix} -2-\delta(\theta), & -2 & , & 3 \\ 24 & , & 4-\delta(\theta), & 1 \\ 8 & , & 26 & , & 5-\delta(\theta) \end{vmatrix}=0,$$

or,

$$\delta(\theta)^3-7\delta(\theta)^2-2012=0.$$

It is thus seen that

$$N[\delta(\theta)]=2012,$$

and

$$\Delta(1,\ \theta,\ \theta^2)=-2^2.503. \tag{3}$$

[1] See Bachmann, p. 280.

Evidently the only prime integer that can divide the index is 2. To see whether 2 is such a divisor, write the function in the form

$$F(x)=x^2(x-1)-2(x+4),$$

so that (Art. 95)

$$P_1(x)=x, \qquad P_2(x)=x-1, \qquad M(x)=x+4.$$

Observe that

$$F(x)=P_1(x)^2P_2(x) \pmod 2,$$

and that $M(x)$ is (mod. 2) divisible by $P_1(x)$, and accordingly the index 2 is a divisor of the index of θ (Art. 95). The discriminant of the realm $\Re(\theta)$ is $D=-503$.

Next write

$$\eta=\tfrac{1}{2}\theta(\theta-1)-1,$$

or

$$2\eta=\theta(\theta-1)-2. \tag{4}$$

Due to the identity (2) we have

$$2\eta\theta=8, \qquad 2\eta\theta^2=8\theta,$$

and by the elimination of θ, it is seen that

$$\eta^3+\eta^2+2\eta-8=0,$$

from which it follows that η is an algebraic integer.

Further, observe that

$$1=1\cdot 1+0\cdot\theta+0\cdot\eta,$$
$$\theta=0\cdot 1+1\cdot\theta+0\cdot\eta,$$
$$\theta^2=2\cdot 1+1\cdot\theta+2\eta,$$

and therefore

$$\Delta(1,\theta,\theta^2)=\begin{vmatrix}1, & 0, & 0\\ 0, & 1, & 0\\ 2, & 1, & 2\end{vmatrix}^2\Delta(1,\theta,\eta).$$

It follows at once that $D=\Delta(1,\theta,\eta)$ and that $1, \theta, \eta$ form a basis of all integers in $\Re(\theta)$.

With this it is seen that any integer γ in $\Re(\theta)$ has the form

$$\gamma=x+\theta y+\eta z,$$

where x, y, z are rational integers. We further have

$$\gamma^2 \equiv x^2 + \theta^2 y^2 + \eta^2 z^2 \pmod 2.$$

From (4) it is seen that

$$\eta^2 = 2\theta - \eta - 2,$$

or

$$\eta^2 \equiv \eta \pmod 2,$$

and

$$\theta^2 \equiv \theta \pmod 2;$$

and therefore also

$$\gamma^2 \equiv \gamma \pmod 2$$

for every integer γ of $\Re(\theta)$.

From this it follows that $\mathfrak{o}2$ is divisible only by the prime ideals of the first degree. For, if f is the degree of any such ideal $\mathfrak{p}$, it would follow that there exist integers τ of $\Re(\theta)$ such that

$$\tau^{2^f} \equiv \tau \pmod{\mathfrak{p}};$$

and since

$$\tau^2 \equiv \tau \pmod{\mathfrak{p}},$$

it is seen in all cases that f, the degree of $\mathfrak{p}$ is 1. Such an ideal can appear only to the first power as a factor of $\mathfrak{o}2$. For, were $\mathfrak{o}2 = \mathfrak{p}^2\mathfrak{q}$, so that $\mathfrak{p}\mathfrak{q}$ is *not* divisible by 2, then there would be an integer, say σ, that is divisible by $\mathfrak{p}\mathfrak{q}$ but *not* by 2 although σ^2 is divisible by 2. But from above, for every integer in $\Re(\theta)$

$$\sigma^2 \equiv \sigma \pmod 2;$$

and, were

$$\sigma^2 \equiv 0 \pmod 2,$$

it would follow also that

$$\sigma \equiv 0 \pmod 2.$$

Accordingly we have

$$\mathfrak{o}2 = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,$$

and that is, the ideal $\mathfrak{o}2$ is *divisible* by the *product* of three prime ideals each of the first degree. To determine

these three ideals, write the fundamental form

$$\xi = u_1 + \theta u_2 + \eta u_3,$$

and observe that the fundamental equation is

$$x^3 - (3u_1 + u_2 - u_3)x^2 + (3u_1^2 + 2u_1u_2 - 2u_1u_3 - 2u_2^2 - 13u_2u_3 + 2u_3^2)x - (u_1^3 + u_1^2u_2 - u_1^2u_3 - 2u_1u_2^2 - 13u_1u_2u_3 + 2u_1u_3^2 + 8u_2^3 - 6u_2^2u_3 + 10u_2u_3^2 + 8u_3^3) = 0.$$

This equation in the form of a congruence is

$$(x+u_1)(x+u_1+u_2)(x+u_1+u_3) \equiv \pmod 2.$$

Writing

$$x = \xi = u_1 + \theta u_2 + \eta u_3,$$

it is seen that

$$\mathfrak{p}_1 = (2,\ \theta,\ \eta),$$
$$\mathfrak{p}_2 = (2,\ \theta+1,\ \eta),$$
$$\mathfrak{p}_3 = (2,\ \theta,\ \eta+1).$$

Finally observe that the number of incongruent (mod. 2) prime functions $P(x)$ is only 2, so that one of the inequalities of Art. 96, must always exist. From this it follows that 2 *is a divisor of the index of every integer* γ *of* $\mathfrak{R}(\theta)$, *where* θ *is defined by the equation* (1).

ART. **100.** A second example of realms in which the index of every integer is divisible by the prime integer $p=2$, is given by Hensel [1] as follows:

THEOREM. *Let* p *be an arbitrary rational prime integer of the form* $p = 3m+1$, *and let* $\mathfrak{G}(\eta)$ *be the Gattung constituted through the three* m*-termed periods of the* p*th roots of unity. The common irregular divisors of the discriminants of all the integers* γ *of this Gattung are to be determined.*

In this connection the reader may well consult Weber's *Algebra*, Vol. I, §§ 180 et seq., and also Burnside and Panton, *Theory of Equations*, 4th Ed., p. 172.

[1] Hensel, *Crelle*, Vol. 113, p. 147.

It was seen in Vol. I, Art. 246, III, that every prime integer p of the form indicated may be written

$$p=(a+b\omega)(a+b\omega^2),$$

where a, $b=3g$ and g are rational integers, and ω is the cube root of unity, namely, $\omega=-\dfrac{1+i\sqrt{3}}{2}$.

It follows that

(1) $$4p=A^2+27B^2,$$

where

$$A=2a-b \qquad \text{and} \qquad 3B=b.$$

For example, if $p=13$,

$$4.13=5^2+27.1$$

and if η is a complex root of $x^{13}-1=0$, the three periods are

$$\eta_0=\eta+\eta^8+\eta^{12}+\eta^5,$$

$$\eta_1=\eta^2+\eta^3+\eta^{11}+\eta^{10},$$

$$\eta_2=\eta^4+\eta^6+\eta^9+\eta^7.$$

It is seen that η_0, η_1, η_2 are the roots of the equation

$$x^3+x^2-4x+1=0.$$

In the general case, see above references, η_0, η_1, η_2 satisfy the equation

(2) $$x^3+x^2-\frac{p-1}{3}x-\frac{1}{9}\left(p\alpha+\frac{p-1}{3}\right)=0,$$

where α is defined through the relation

$$3\alpha=A+2.$$

Accordingly, the different of η_0 is

$$\delta(\eta_0)=3\eta_0^2+2\eta_0-\frac{p-1}{3},$$

and

$$\eta_0\delta(\eta_0)=-\eta_0^2+2\frac{p-1}{3}\eta_0+3C,$$

$$\eta_0^2\delta(\eta_0)=\left(1+2\frac{p-1}{3}\right)\eta_0^2+\left(3C-\frac{p-1}{3}\right)\eta_0-C,$$

where

$$C=\frac{1}{9}\left(p\alpha+\frac{p-1}{3}\right).$$

It follows (Vol. I, Arts. 94 and 104) that

$$-\Delta(1,\ \eta_0,\ \eta_0^2)=\begin{vmatrix} 3, & 2, & -\frac{p-1}{3} \\ -1, & 2\frac{p-1}{3}, & 3C \\ 1+2\frac{p-1}{3}, & 3C-\frac{p-1}{3}, & -C \end{vmatrix},$$

or

$$-\Delta(1,\ \eta_0,\ \eta_0^2)=\frac{4p^2m+4p^2\alpha-3p^2\alpha^2}{9}.$$

We accordingly have

$$\Delta(1,\ \eta_0,\ \eta_0^2)=-B^2p^2.$$

Observe on the other hand that

$$1=-\eta_0-\eta_1-\eta_2,$$

$$\eta_0=1\cdot\eta_0+0\cdot\eta_1+0\eta_2,$$

$$-\eta_0^2=\left(\frac{p-1}{3}-m_0^0\right)\eta_0+\left(\frac{p-1}{3}-m_1^0\right)\eta_1+\left(\frac{p-1}{3}-m_2^0\right)\eta_2,$$

where[1] $m_0^0,\ m_1^0,\ m_2^0$ are three rational integers, which satisfy the equation

$$m_1^0-m_2^0=B.$$

From these three relations it follows that

$$\Delta(1,\ \eta_0,\ \eta_0^2)=\begin{vmatrix} -1, & -1, & -1 \\ 1, & 0, & 0 \\ \frac{p-1}{3}-m_0^0, & \frac{p-1}{3}-m_1^0, & \frac{p-1}{3}-m_2^0 \end{vmatrix}^2\Delta(\eta_0,\ \eta_1,\ \eta_2),$$

or

$$\Delta(1,\ \eta_0,\ \eta_0^2)=B^2\Delta(\eta_0,\ \eta_1,\ \eta_2).$$

Hence, from above it is seen that

$$\Delta(\eta_0,\ \eta_1,\ \eta_2)=-p^2.$$

[1] Bachmann, *Die Lehre von der Kreisteilung*, p. 201.

Since the discriminant of every realm (Art. 298) is different from ± 1, it is seen that $-p^2$ is the discriminant (basal invariant) of the realm $\Re(\eta)$, while η_0, η_1, η_2 are a basis of all the integers (of the order-modul o) of this realm.

The fundamental form is accordingly

$$\xi = \eta_0 u_0 + \eta_1 u_1 + \eta_2 u_2, \text{ with conjugate values}$$
$$\xi' = \eta_1 u_0 + \eta_2 u_1 + \eta_0 u_2,$$
$$\xi'' = \eta_2 u_0 + \eta_0 u_1 + \eta_1 u_2;$$

while the discriminant of the fundamental equation is

$$(\xi - \xi')^2(\xi' - \xi'')^2(\xi'' - \xi)^2 = H_1 U_2 - H_2 U_1,$$

where

$$U_1 = u_0 u_1^2 + u_1 u_2^2 + u_2 u_0^2 - u_0^2 u_1 - u_1^2 u_2 - u_2^2 u_0,$$
$$U_2 = u_0^3 + u_1^3 + u_2^3 + 6 u_0 u_1 u_2 - 3(u_0 u_1^2 + u_1 u_2^2 + u_2 u_0^0),$$
$$H_1 = \eta_0 \eta_1^2 + \eta_1 \eta_2^2 + \eta_2 \eta_0^2 - \eta_0^2 \eta_1 - \eta_1^2 \eta_2 - \eta_2^2 \eta_0,$$
$$H_2 = \eta_0^3 + \eta_1^3 + \eta_2^3 + 6 \eta_0 \eta_1 \eta_2 - 3(\eta_0 \eta_1^2 + \eta_1 \eta_2^2 + \eta_2 \eta_0^2).$$

If the η's, as symmetric functions of the roots, are expressed through the coefficients of the equation (2), this discriminant takes the form

$$-p(aU_1 + BU_2).$$

In Art. 76 it was seen that

$$\Delta(1, \xi, \xi^2) = D\vartheta(u_0, u_1, u_2)^2,$$

so that here

$$\vartheta(u_0, u_1, u_2) = aU_1 + BU_2.$$

Observe next that

$$U_1 \equiv 0 \pmod 2,$$

while

$$U_2 \equiv u_0 + u_1 + u_2 + u_0 u_1 + u_1 u_2 + u_2 u_0 \pmod 2.$$

It follows that

$$\vartheta(u_0, u_1, u_2) \equiv B(u_0 + u_1 + u_2 + u_0 u_1 + u_1 u_2 + u_2 u_0) \pmod 2.$$

Hence, only when $B \equiv 0 \pmod 2$, is $\vartheta(u_0, u_1, u_2)$ divisible

by 2 for indeterminate values of u_0, u_1, u_2. In this case it follows from (1) that A must be divisible by 2 and therefore also that

$$p = A'^2 + 27B'^2. \tag{3}$$

From this it is seen that the rational integer 2 is an irregular divisor of the discriminant of every integer γ in $\mathfrak{R}(\eta)$, if the prime integer $p = 3m+1$ is of the form (3). It is clear that this is true of the integers

$$p = 31,\ 43,\ 109,\ 127,\ 157,\ 189,\ \cdots.$$

See also the example given by Dedekind, *Gött. gelehrten Anzeigen*, Sept. 20, 1871.

ART. **101.** Kronecker (*Grundzüge*) called attention to a supposed fact that although the index $\vartheta(u_1, u_2, \cdots, u_n)$ for certain realms was divisible by a definite prime integer p, when the indeterminates $u_1, u_2, \cdots, u_n$ ran through all rational integers, the same was *not* true when instead of the rational integers, the algebraic integers of determinate definite algebraic realms were written for the u's. This conjecture of Kronecker was later proved by Hensel,[1] who, by making an interesting application of modular systems, also determined the realms of lowest degree whose integers, when written for the u's, offered indices that were *not* divisible by a prime integer p.

Hensel made use of the following theorem, which may be proved in a similar manner as the theorem of Vol. I, Art. 202:

Let

$$F_1(u_1),\ F_2(u_2),\ \cdots,\ F_n(u_n) \tag{1}$$

be n rational integral functions with integral coefficients, each being of one variable, and suppose (mod. p) that each function $F_i(u_i)$ has as many incongruent integral roots ρ_i as the degree of the function. Further, let $F(u_1, u_2, \cdots, u_n)$

[1] Hensel, *Crelle's Journal*, Vol. 113, p. 149.

be a rational integral function with rational integral coefficients of all the quantities $u_1, u_2, \cdots, u_n$. *The congruence*

$$F(\rho_1, \rho_2, \cdots, \rho_n) \equiv 0 \pmod{p} \tag{2}$$

exists then and only then for all the roots of the congurences

$$F_i(u_i) \equiv 0 \pmod{p} \qquad (i = 1, 2, \cdots, n),$$

if $F(u_1, u_2, \cdots, u_n)$ *is contained in the modular system*

$$(p, F_1(u), \cdots, F_n(u)).$$

Further, if $\Re(\alpha)$ is any algebraic realm and if $\mathfrak{p}$ is a prime ideal divisor of p in this realm, the more general theorem may be proved; namely, that *a function* $F(u_1, u_2, \cdots, u_n)$, *whose coefficients are integers of* $\Re(\alpha)$, *is then and only then divisible by* $\mathfrak{p}$, *when for* $u_1, \cdots, u_n$ *are written all the roots of the congruences*

$$F_1(u_1) \equiv 0, \quad F_2(u_2) \equiv 0, \quad \cdots, \quad F_n(u_n) \equiv 0 \pmod{\mathfrak{p}}, \tag{3}$$

if it is contained in the modular system [1]

$$(\mathfrak{p}, F_1(u_1), \cdots, F_n(u_n)),$$

where each function $F_i(u_i)$ *has integral coefficients that belong to* $\Re(\alpha)$ *and has as many integral roots* (*mod.* p) *as the degree of the function.*

The proof of this theorem will be given under the special assumption that the functions F and $F_i (i = 1, 2, \cdots, n)$ have rational integral coefficients. We may then reduce F with respect to the modular system $(F_1, F_2, \cdots, F_n)$. The resulting remainder is likewise a rational integral function in $u_1, u_2, \cdots, u_n$ with rational integral coefficients, and may accordingly be divided by $\mathfrak{p}$, only if it is divisible by p.

Under this particular assumption it follows that *the function* $F(u_1, u_2, \cdots, u_n)$ *is divisible by* $\mathfrak{p}$ *for all systems of roots of the congruences* (3), *if and only if it is contained*

[1] Modular systems, in which ideals enter as elements, have been treated in an extensive paper by the author "Mémoire sur les systèmes modulaires de Kronecker," *L'École Normale Supérieure*, Vol. 18, 1901.

in the modular system

$$(p, F_1(u_1), F_2(u_2), \cdots, F_n(u_n)).$$

Next, let the prime ideal $\mathfrak{p}$ be of degree f, and that is

$$N(\mathfrak{p}) = p^f.$$

It was seen in Art. 38 that the congruences

$$u_1^{p^f} - u_1 \equiv 0,\ u_2^{p^f} - u_2 \equiv 0,\ \cdots,\ u_n^{p^f} - u_n \equiv 0 \pmod{\mathfrak{p}}$$

have as many incongruent (mod. $\mathfrak{p}$) roots, which are integers of the realm, as is the degree of $\mathfrak{p}$, and that is p^f, and this is the number of incongruent (mod. $\mathfrak{p}$) integers of the realm.

It is seen that if instead of the functions

$$F_i(u_i) \qquad (i=1, 2, \cdots, n)$$

above, we write the functions

$$u_i^{p^f} - u_i \qquad (i=1, 2, \cdots, n),$$

we have from the preceding, the following theorem:

In order that the function $\vartheta(u_1, u_2, \cdots, u_n)$ be divisible by $\mathfrak{p}$ for all systems of integers of the realm $\Re(\alpha)$, it is necessary and sufficient that it be contained in the modular system

$$(p, u_1^{p^f} - u_1, u_2^{p^f} - u_2, \cdots, u_n^{p^f} - u_n).$$

If the function ϑ is not contained in this system, there exists a system of integers $\alpha_1, \alpha_2, \cdots, \alpha_n$ of the realm $\Re(\alpha)$, such that $\vartheta(\alpha_1, \alpha_2, \cdots, \alpha_n)$ is *not* divisible by $\mathfrak{p}$.

Suppose next that p, when factored in $\Re(\alpha)$, takes the form

$$p = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2} \cdots \mathfrak{p}_r^{a_r},$$

where the degrees of $\mathfrak{p}_i$ are respectively f_i $(i=1, 2, \cdots, r)$. Write down the modular systems

$$M_i = [p, u_1^{p^{f_i}} - u_1, u_2^{p^{f_i}} - u_2, \cdots, u_n^{p^{f_i}} - u_n] \qquad (i=1, 2, \cdots, r), \tag{4}$$

where these systems are not necessarily different. For example, $M_1 = M_2$, if $f_1 = f_2$. It is clear from the above,

if the function $\vartheta(u_1, u_2, \cdots, u_n)$ is contained in any one of these modular systems, that p is a common irregular divisor of the discriminants of the integers of $\Re(\alpha)$. Accordingly, the necessary and sufficient condition that p be *not* an irregular divisor, is that ϑ be *not* contained in any of the above modular systems. For this condition to be satisfied, there exist systems of values $\alpha_1^{(i)}, \alpha_2^{(i)}, \cdots, \alpha_n^{(i)}$ for each $\mathfrak{p}_i$ $(i=1, 2, \cdots, r)$ of the realm $\Re(\alpha)$, such that $\vartheta(\alpha_1^{(i)}, \alpha_2^{(i)}, \cdots, \alpha_n^{(i)})$ is *not* divisible by $\mathfrak{p}_i$. For (Art. 33), we may choose integers $\alpha_1, \alpha_2, \cdots, \alpha_n$ of $\Re(\alpha)$, such that

$$\alpha_k \equiv \alpha_k^{(1)} \text{ (mod. } \mathfrak{p}_1), \alpha_k \equiv \alpha_k^{(2)} \text{ (mod. } \mathfrak{p}_2), \cdots, \alpha_k \equiv \alpha_k^{(r)} \text{ (mod. } \mathfrak{p}_r) \quad (k=1, 2, \cdots, n).$$

It follows that

$$\vartheta(\alpha_1, \alpha_2, \cdots, \alpha_n) \equiv \vartheta(\alpha_1^{(i)}, \alpha_2^{(i)}, \cdots, \alpha_n^{(i)}) \text{ (mod. } \mathfrak{p}_i) \quad (i=1, 2, \cdots, r);$$

and therefore it follows also, as $\vartheta(\alpha_1, \alpha_2, \cdots, \alpha_n)$ is divisible by none of the $\mathfrak{p}$'s, that it is *not* divisible by p.

The above results may be expressed through the theorem: *In order that the function* $\vartheta(u_1, u_2, \cdots, u_n)$ *be not divisible by a rational prime integer* p, *when for the indeterminates* $u_1, u_2, \cdots, u_n$ *are written all systems of the algebraic integers of a realm* $\Re(\alpha)$, *it is necessary and sufficient that this function be not contained in any of the modular systems* (4).

A realm $\Re(\theta)$ which has this property was called by Hensel (*op. cit.*, p. 153) a *complete* (*Erganzungs*) realm. To prove the existence of such Henselian realms and to determine those of the lowest degree, we may proceed as follows:

Write the systems

$$M_i = [p, u_1^{p^i} - u_1, u_2^{p^i} - u_2, \cdots, u_n^{p^i} - u_n] \quad (i=1, 2, \cdots),$$

and observe, when i is taken sufficiently large, that there

is a system M_i which does not contain as an element $\vartheta(u_1, \cdots, u_n)$. For, note that the dimensions of this function in $u_1, u_2, \cdots, u_n$ are $\frac{n(n-1)}{2}$. If then k is the smallest integer for which $p^k > \frac{n(n-1)}{2}$, it is clear that $D(u_1, u_2, \cdots, u_n)$ is not contained in M_k unless $\vartheta(u_1, u_2, \cdots, u_n)$ is divisible by p. It was shown in Art. 76 that ϑ is a unit-form and therefore *not* divisible by p.

Suppose that M_g is the first of the modular system which does not contain $\vartheta(u_1, u_2, \cdots, u_n)$ and take any irreducible congruence $P(x) \equiv 0 \pmod{p}$ of the gth degree. If α is any root of the equation $P(x) = 0$, it may be shown that $\Re(\alpha)$ is a Henselian realm for the prime integer p. For (see note at end of this article) it may be shown (Art. 95) that p is not factorable in $\Re(\alpha)$, so that the degree of the ideal $\mathfrak{o}p$ in this realm is g; and from above, M_g does not contain $\vartheta(u_1, u_2, \cdots, u_n)$. It may be shown further that there is no complete (*Erganzungs*) realm of less degree than the degree of $\Re(\alpha)$. For, were $\Re(\beta)$ such, where $k < g$, and if $\mathfrak{p}$ is a prime ideal factor of p in this realm, its degree can at most be equal to k. But, since by hypothesis, $\vartheta(u_1, u_2, \cdots, u_n)$ is contained in every modular system M_i, where $i \gtrless k$, it follows from above that $\mathfrak{p}$ is a divisor of all values of the function $\vartheta(u_1, u_2, \cdots, u_n)$, when for the u's are written any system of integral values of the realm $\Re(\beta)$.

Observe next that the congruence (Art. 38)

$$x^{p^f} - x \equiv 0 \pmod{\mathfrak{p}}$$

takes here the form

$$x^{p^g} - x \equiv 0 \pmod{p}, \tag{5}$$

so that there are $p^g [= N(\mathfrak{o}p)]$ incongruent (mod. p) integers of $\Re(\alpha)$. Further, if $\Re(\gamma)$ is another complete

realm of the gth degree, whose systems of integers when written for the indeterminates u_i in $\vartheta(u_1, \cdots, u_n)$, offer quantities that are not divisible by p, it would follow that there are also p^g incongruent (mod. p) integers of this realm, which, however, are roots of the congruence (5) and are therefore quantities of $\Re(\alpha)$. It follows that the realms $\Re(\alpha)$ and $\Re(\gamma)$ are equivalent.

It is thus seen that the choice of the prime function $P(x)$ (mod. p) of degree g, whose root is to form the complete realm, is arbitrary. Hensel (*loc. cit.*) further extends this theory by making the roots of unity generate Henselian realms for fixed prime rational integers p.

Note. It may be proved that p is *not* factorable in the realm $\Re(\alpha)$ above. For it is evident as in Art. 62 that every integer of $\Re(\alpha)$ may be expressed linearly through $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ with rational integral coefficients. Hence, if $\mathfrak{o}p = \mathfrak{p}\mathfrak{q}$, there are integers τ, σ in $\Re(\alpha)$, such that

$$\tau = \tau(\alpha) \equiv 0 \text{ (mod. } \mathfrak{p}), \qquad \sigma = \sigma(\alpha) \equiv 0 \text{ (mod. } \mathfrak{q}),$$
$$\tau \not\equiv 0 \text{ (mod. } p), \qquad \sigma \not\equiv 0 \text{ (mod. } p),$$

and

$$\tau\sigma \equiv 0 (\text{mod. } p).$$

It follows (Art. 61) that

$$\tau(x)\sigma(x) \equiv 0 \text{ (modd. } p, P(x)),$$

which leads to the contradiction that either τ or σ is divisible by p.

EXAMPLE. It was proved (Art. 99) that 2 is a divisor of the indices of all integers γ of the realm defined through the equation

$$x^3 - x^2 - 2x - 8 = 0.$$

Show that in the extended realm, made by adjoining the cube root of unity to this realm, the integer 2 is no longer such an irregular divisor. (Kronecker.)

II. The Regular Divisors. The Fundamental Ideal

Art. **102.** In Art. 92 a proof was given by Hensel that the discriminant or fundamental invariant D of a fixed realm or Gattung $\mathfrak{R}(\alpha)$ is composed entirely of those prime integers p as factors which themselves have as factors prime ideals to a power higher than the first.

This Dedekind theorem was also proved in Arts. 31 and 77. A somewhat different proof with further consequences will be given here:[1]

Theorem. *Every rational prime integer p, which is divisible by the square of a prime ideal, is a divisor of D.*

For, suppose that $\mathfrak{o}p = \mathfrak{p}^2\mathfrak{q}$. It is possible (Vol. I, Art. 215) to find an integer γ of the ideal $\mathfrak{p}\mathfrak{q}$ such that

$$\gamma = c_1\omega_1 + c_2\omega_2 + \cdots + c_n\omega_n,$$

which is *not* divisible by $\mathfrak{p}\mathfrak{q}$ (or p), and in which the coefficients c are not all divisible by p.

On the other hand

$$\gamma^2 = \mathfrak{p}^2\mathfrak{q}^2$$

is divisible by p, so that

$$\gamma^p \equiv c_1\omega_1^p + c_2\omega_2^p + \cdots + c_n\omega_n^p \equiv 0 \pmod{p};$$

and also for the conjugate values there exist the congruences,

$$\begin{aligned} c_1\omega_1^{(1)p} + c_2\omega_2^{(1)p} + \cdots + c_n\omega_n^{(1)p} &\equiv 0 \pmod{p}, \\ \cdots\cdots\cdots\

we observe that (Vol. I, Art. 104)

$$D=\begin{vmatrix} S(\omega_1\omega_1), & S(\omega_1\omega_2), & \cdots, & S(\omega_1\omega_n) \\ S(\omega_2\omega_1), & S(\omega_2\omega_2), & \cdots, & S(\omega_2\omega_n) \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ S(\omega_n\omega_1), & S(\omega_n\omega_2), & \cdots, & S(\omega_n\omega_n) \end{vmatrix},$$

and that

$$\begin{aligned} S(\gamma)^p &= (\gamma^{(1)}+\gamma^{(2)}+\cdots+\gamma^{(n)})^p \\ &\equiv \gamma^{(1)p}+\gamma^{(2)p}+\cdots+\gamma^{(n)p} \\ &\equiv S(\gamma^p) \pmod{p}. \end{aligned}$$

Accordingly, it follows that

$$D\equiv 0 \pmod{p}.$$ (See also p. 62.)

ART. 103. The inverse of the above theorem may next be proved, namely: THEOREM. *Every prime integer p which is a divisor of D is itself divisible by the square of a prime ideal.* (Dedekind, *Werke*, Vol. I, pp. 356 ff.)

Let $\mathfrak{R}(\alpha)$ be the fixed realm of the nth degree and write D in the form of the determinant of the preceding article. Observe that the elements of that determinant are rational integers. It follows, when this determinant is congruent to zero (mod. p), that there exist rational integers $x_1, x_2, \cdots, x_n$, which are not all divisible by p, such that the following n congruences

$$x_1S(\omega_1\omega_i)+x_2S(\omega_2\omega_i)+\cdots+x_nS(\omega_n\omega_i)\equiv 0 \pmod{p} \qquad (i=1, 2, \cdots, n)$$

are satisfied. If the integer γ has the fixed value

$$\gamma=x_1\omega_1+x_2\omega_2+\cdots+x_n\omega_n,$$

the above congruences become

$$S(\gamma\omega_i)\equiv 0 \pmod{p} \qquad (i=1, 2, \cdots, n).$$

And, if these n congruences are multiplied respectively by any rational integers $z_1, z_2, \cdots, z_n$ and added, there exists for every integer of the realm

$$\tau=\omega_1z_1+\omega_2z_2+\cdots+\omega_nz_n$$

the congruence

$$S(\gamma\tau) \equiv 0 \pmod{p}.$$

If η is any other integer of the realm, this congruence may be given the somewhat more general form

$$S(\gamma\tau + p\eta) \equiv 0 \pmod{p}. \tag{1}$$

Observe next that the collectivity of integers $\gamma\tau + p\eta$, where τ and η go over all the integers of the fixed realm $\Re(\alpha)$, constitute an ideal i which is the greatest common ideal-divisor of the two ideals $\mathfrak{o}\gamma$ and $\mathfrak{o}p$. Since the n integers $x_1, x_2, \cdots, x_n$ are not all divisible by p, it follows that the fixed integer γ is *not* divisible by p, and accordingly does not belong to the ideal $\mathfrak{o}p$, and therefore also i is a divisor of the ideal $\mathfrak{o}p$ and is different from $\mathfrak{o}p$. And that is, $\mathfrak{o}p > \mathfrak{i}$, while i is *not* divisible by $\mathfrak{o}p$.

If then we assume that *the ideal* $\mathfrak{o}p$ *is factorable into prime ideal factors that are all different from one another, there is at least one of these factors, say* $\mathfrak{p}$, *which is* not *a divisor of* i. *Otherwise* i *would be divisible by* p.

Writing $p = \mathfrak{p}\mathfrak{q}$, it follows that $\mathfrak{q}$ is divisible by i. And as every integer κ of $\mathfrak{q}$ is divisible by i, it follows from (1) that

$$S(\kappa) \equiv 0 \pmod{p}. \tag{2}$$

Under the assumption that p is factorable into ideal factors that are all different, it is thus proved that the prime integer p is factorable into two ideal factors $\mathfrak{p}\mathfrak{q}$ of which the one is *not* divisible by i, while every integer κ of the second ideal satisfies the congruence (2). If we prove that this leads to a contradiction, it follows that p must be divisible by the square of at least one prime ideal. With the proof of this the theorem is established.

To prove this contradiction, write (see Art. 65)

$$\mathfrak{p} = (p, P(\rho)),$$

and observe:

First. If f is the degree of the ideal $\mathfrak{p}$ and (Art. 72) $P(x)$ an irreducible function (mod. p) of degree f, then

also $P(x)=0$ is an irreducible equation of the fth degree. Let σ be a root of this equation and $\Re(\sigma)$ the realm generated by σ. Denote the order-modul, discriminants, norms, spurs, etc., of this new realm by $\mathfrak{o}_1$, Δ_1, N_1, S_1, etc. Due to the identity $P(\sigma)=0$, every power of σ may be written in the form

$$\sigma^m = c_0^{(m)} + c_1^{(m)}\sigma + \cdots + c_{f-1}^{(m)}\sigma^{f-1}; \tag{3}$$

and due to the irreducibility of the equation $P(x)=0$, (Vol. I, Art. 44)

$$x^m = c_0^{(m)} + c_1^{(m)}x + \cdots + c_{f-1}^{(m)}x^{f-1} + P(x)Q(x), \tag{4}$$

where $Q(x)$ is an integral function of x with rational integral coefficients.

From (3) above we have at once

$$\begin{aligned}
1\cdot\sigma^m &= c_0^{(m)}\cdot 1 + c_1^{(m)}\sigma + \cdots + c_{f-1}^{(m)}\sigma^{f-1},\\
\sigma\cdot\sigma^m &= c_0^{(m+1)}\cdot 1 + c_1^{(m+1)}\sigma + \cdots + c_{f-1}^{(m+1)}\sigma^{f-1},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
\sigma^{f-1}\cdot\sigma^m &= c_0^{(m+f-1)}\cdot 1 + c_1^{(m+f-1)}\cdot\sigma + \cdots + c_{f-1}^{(m+f-1)}\cdot\sigma^{f-1}.
\end{aligned}$$

From these relations, since $1, \sigma, \sigma^2, \cdots, \sigma^{f-1}$ constitute a basis of $\Re(\sigma)$, may be derived (Vol. I, Art. 59) the spur of σ^m in the form

$$S(\sigma^m) = S_m,$$

where

$$S_m = c^{(m)} + c_1^{(m+1)} + \cdots + c_{f-1}^{(m+f-1)}.$$

Next observe that on the one hand

$$\begin{aligned}
\Delta_1(\sigma) &= \Delta_1(1, \sigma, \cdots, \sigma^{(f-1)})\\
&= \begin{vmatrix} S_1(1), & S_1(\sigma), & \cdots, & S_1(\sigma^{f-1}) \\ S_1(\sigma), & S_1(\sigma^2), & \cdots, & S_1(\sigma^f) \\ \cdots\cdots & \cdots\cdots & \cdots & \cdots\cdots \\ S_1(\sigma^{f-1}), & S_1(\sigma^f), & \cdots, & S_1(\sigma^{2f-2}) \end{vmatrix}\\
&= \begin{vmatrix} S_0, & S_1, & \cdots, & S_{f-1} \\ S_1, & S_2, & \cdots, & S_f \\ \cdots\cdots & \cdots\cdots & \cdots & \cdots\cdots \\ S_{f-1}, & S_f, & \cdots, & S_{2f-2} \end{vmatrix} = S, \text{ say.}
\end{aligned}$$

On the other hand (Vol. I, Art. 63)

$$\Delta_1(\sigma) = (-1)^{\frac{f(f-1)}{2}} N_1(P'(\sigma)).$$

Since $P'(x)$ and $P(x)$ are (mod. p) relatively prime (Vol. I, Art. 41), it is seen that

$$P(x)\Phi(x) + P'(x)\Psi(x) \equiv 1 \pmod{p}.$$

It follows that

$$P'(\sigma)\Psi(\sigma) \equiv 1 \pmod{p},$$

and consequently $P'(\sigma)$ is *not* divisible by p. It follows also (Vol. I, Art. 89) that $N_1(P'(\sigma))$ is not divisible by p, and that is, $S = \Delta_1(\sigma)$ is *not* divisible by p.

Secondly. The number ρ was a root of the congruence (Art. 61)

$$P(x) \equiv 0 \pmod{\mathfrak{p}}.$$

We further saw (Art. 62) that a congruence

$$a_0 + a_1\rho + \cdots + a_{f-1}\rho^{f-1} \equiv 0 \pmod{\mathfrak{p}} \tag{5}$$

was impossible, and therefore also this same congruence was impossible (mod. p) unless all the rational integers a_i were divisible by p.

Due to the assumption that in the fixed realm $\Re(\alpha)$ the ideal factors of p were all different, it is seen that if we write $p = \mathfrak{p}\mathfrak{q}$, that the two ideals $\mathfrak{p}$ and $\mathfrak{q}$ are relatively prime. We may accordingly (Art. 33) determine an integer τ of the fixed realm such that

$$\tau \equiv 1 \pmod{\mathfrak{p}}, \qquad \tau \equiv 0 \pmod{\mathfrak{q}};$$

and therefore

$$\tau^2 \equiv \tau \pmod{p}. \tag{6}$$

Writing

$$\kappa_1 = \tau \cdot 1, \ \kappa_2 = \tau \cdot \rho, \ \cdots, \ \kappa_f = \tau\rho^{f-1}, \tag{7}$$

it is seen that each of these f quantities is divisible by $\mathfrak{q}$, and, due to the impossibility of the relation (5), these quantities are (mod. p) independent; and that is, a

relation

$$c_1\kappa_1+c_2\kappa_2+\cdots+c_f\kappa_f\equiv 0 \pmod{p}$$

does not exist, unless all the c's are divisible by p. However, more than f (mod. p) independent integers that are divisible by $\mathfrak{q}$ do *not* exist. For, were $\kappa_1, \kappa_2, \cdots, \kappa_{f+1}$ such integers that

$$c_1\kappa_1+c_2\kappa_2+\cdots+c_{f+1}\kappa_{f+1}\equiv 0 \pmod{p},$$

it would follow that this congruence existed (mod. $\mathfrak{p}$), and this is not true.

It follows as in Art. 62 that every integer κ in $\mathfrak{q}$ may be written

$$\kappa\equiv a_1\kappa_1+a_2\kappa_2+\cdots+a_f\kappa_f \pmod{p},$$

where the a's are rational integers.

Further, if g is the number of integers of $\mathfrak{p}$ that are linearly independent (mod. p), and if $\tilde{\omega}_1, \tilde{\omega}_2, \cdots, \tilde{\omega}_g$ are such numbers, then every number $\tilde{\omega}$ in $\mathfrak{p}$ may be written

$$\tilde{\omega}=b_1\tilde{\omega}_1+b_2\tilde{\omega}_2+\cdots+b_g\tilde{\omega}_g \pmod{p},$$

where the b's are rational integers, which like the a's are not all divisible by p. Further, as $\mathfrak{p}$ and $\mathfrak{q}$ are relatively prime, the $f+g$ integers

$$\kappa_1, \kappa_2, \cdots, \kappa_f, \tilde{\omega}_1, \tilde{\omega}_2, \cdots, \tilde{\omega}_g$$

are (mod. p) linearly independent; and that is, an integral congruence

$$(8)\quad a_1\kappa_1+a_2\kappa_2+\cdots+a_f\kappa_f+b_1\tilde{\omega}_1+\cdots+b_g\tilde{\omega}_g\equiv 0 \pmod{p}$$

can only exist if all the a's and b's are divisible by p. For, since the κ's are all divisible by $\mathfrak{q}$, it would follow from the above congruence that

$$b_1\tilde{\omega}_1+b_2\tilde{\omega}_2+\cdots+b_g\tilde{\omega}_g\equiv 0 \pmod{\mathfrak{q}};$$

and since the left hand side of this congruence is an integer that is divisible by $\mathfrak{p}$, it follows also that

$$b_1\tilde{\omega}_1+b_2\tilde{\omega}_2+\cdots+b_g\tilde{\omega}_g\equiv 0 \pmod{p}$$

which congruence requires that all the b's be divisible by

p. And, taking the congruence (8) with respect to $\mathfrak{q}$, the other divisor of p, it follows that the a's are all divisible by p.

Since $\mathfrak{o}=\mathfrak{p}+\mathfrak{q}$, it is seen that every integer ζ of the realm $\Re(\alpha)$ may be expressed through the integral congruence

$$\zeta=a_1\kappa_1+a_2\kappa_2+\cdots+a_f\kappa_f+b_1\tilde{\omega}_1+\cdots+b_g\tilde{\omega}_g\equiv 0 \pmod{p}.$$

Letting the a's and b's go through all integral values 0, 1, $\cdots$, $p-1$, it is seen that in $\mathfrak{o}$ there are p^{f+g} integers ζ that are incongruent (mod. p). But this number is (Art. 11)

$$(\mathfrak{o},\ \mathfrak{o}p)=N(\mathfrak{o}p)=p^n.$$

It follows that

$$n=f+g.$$

If $\omega_1, \omega_2, \cdots, \omega_n$ form a basis of all integers of $\mathfrak{o}$, the quantities $\kappa_1, \cdots, \kappa_f, \tilde{\omega}_1, \cdots, \tilde{\omega}_g$ may be expressed linearly through the basal elements $\omega_1, \cdots, \omega_n$. If C is the determinant of these n linear relations, it follows that the ω's may be expressed as linear forms of the κ's and $\tilde{\omega}$'s, each linear form being divided by C. Accordingly, any integer η of $\mathfrak{o}$ multiplied by C may be expressed linearly in terms of the κ's and $\tilde{\omega}$'s in the form (the r's denoting rational integers)

$$C\eta=r_1\kappa_1+r_2\kappa_2+\cdots+r_f\kappa_f+r_{f+1}\tilde{\omega}_1+\cdots+r_n\tilde{\omega}_g \pmod{p}.$$

Due to the linear independence (mod. p) of the κ's and $\tilde{\omega}$'s on the right hand side of this expression, it is seen that the *determinant C is* not *divisible by p.*

Thirdly. Writing $x=\rho$ in equation (4) and multiplying the resulting expression by τ, the congruence

$$\tau\rho^m\equiv c_0^{(m)}\kappa_1+c_1^{(m)}\kappa_2+\cdots+c_{f-1}^{(m)}\kappa_f \pmod{\mathfrak{p}} \tag{9}$$

follows at once from the relations (7). The integer on the right hand of this congruence being divisible by $\mathfrak{q}$, it is seen that this congruence also exists, modulo p.

Observe next that [see formulas (6) and (7)]

$$\kappa_i \tau \rho^m = \tau^2 \rho^{m+i-1} \equiv \tau \rho^{m+i-1} \pmod{\mathfrak{p}}.$$

Hence, using the formula (9), we have the following congruences (mod. p):

$$\begin{aligned}
\kappa_1 \tau \rho^m &\equiv C_0^{(m)} \kappa_1 + C_1^{(m)} \kappa_2 + \cdots + C_{f-1}^{(m)} \kappa_f, \\
\kappa_2 \tau \rho^m &\equiv C_0^{(m+1)} \kappa_1 + C_1^{(m+1)} \kappa_2 + \cdots + C_{f-1}^{(m+1)} \kappa_f, \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
\kappa_f \tau \rho^m &\equiv C_0^{(m+f-1)} \kappa_1 + C_1^{(m+f-1)} \kappa_2 + \cdots + C_{f-1}^{(m+f-1)} \kappa_f.
\end{aligned}$$

Observe next that the quantities $\tilde{\omega}_i$ are all divisible by $\mathfrak{p}$, while the quantity $\tau \rho^m$ is divisible by $\mathfrak{q}$. Accordingly, the integers $\tilde{\omega}_i \tau \rho^m$ $(i = 1, 2, \cdots, g)$ are all divisible by p.

It follows that in addition to the f congruences above, we have the g congruences (mod. p):

$$\begin{aligned}
\tilde{\omega}_1 \tau \rho^m &\equiv 0 \pmod{p}, \\
\tilde{\omega}_2 \tau \rho^m &\equiv 0 \pmod{p}, \\
&\cdots\cdots\cdots\cdots \\
\tilde{\omega}_g \tau \rho^m &\equiv 0 \pmod{p}.
\end{aligned}$$

These n congruences may be written in the form of equations, if to the right hand side of each of them is added $p\zeta_i$, where $Cp\zeta_i$ is, from above, an expression of the form

$$p(a_{1i}\kappa_1 + a_{2i}\kappa_2 + \cdots + a_{fi}\kappa_f + b_{1i}\tilde{\omega}_1 + \cdots + b_{gi}\tilde{\omega}_g) \qquad (i = 1, 2, \cdots, n).$$

It follows (Vol. I, Art. 59) that

$$S(C\tau\rho^m) \equiv C(c_0^{(m)} + c_1^{(m+1)} + \cdots + c_{f-1}^{(m+f-1)}) \pmod{p};$$

or, since $C \not\equiv 0 \pmod{p}$, that

$$S(\tau\rho^m) \equiv S_m \pmod{p}.$$

Observe next (formula (7)) that $\tau\rho^m$ is divisible by $\mathfrak{q}$ and from formula (2), the spur of such a number is divisible by p. It would therefore follow that

$$S_m \equiv 0 \pmod{p},$$

and therefore S would be divisible by p, which contradicts what was found in the first heading.

ART. **104.** To get the full import of the fundamental invariant D, the discriminant of the realm, and at the same time to emphasize again and from a different point of view, some of the results that have already been indicated as fundamental, it is well to develop here the work of Dedekind (§§ 7–14 of the paper "Ueber die Discriminanten endlichen Körper," *Göttingen Abh.*, Vol. 29; *Werke*, Vol. I, pp. 351 ff.).

Let θ be an integer which satisfies the irreducible equation

$$F(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0$$

of the nth degree, where the a's are rational integers; and form the realm $\Re(\theta)$.

Every rational integral function of θ with rational integral coefficients may be written (Vol. I, Art. 44)

$$\varphi(\theta) = c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1},$$

where the c's are rational integers (including zero). Accordingly, the collectivity of such functions is identical with the modul (see also Bachmann, p. 303)

$$\mathfrak{o}_1 = [1, \theta, \theta^2, \cdots, \theta^{n-1}],$$

which modul, due to the identity $F(\theta) = 0$, is a ring modul in $\Re(\theta)$, since the product of any two functions in it is a function of it; and that is,

$$\mathfrak{o}_1\mathfrak{o}_1 = \mathfrak{o}_1;$$

and further, it contains the unit modul $\mathfrak{z} = [1]$. The ring leader (Vol. I, Art. 237) of this order-modul may be denoted by $\mathfrak{f}$, where

$$\mathfrak{f} = \frac{\mathfrak{o}_1}{\mathfrak{o}}$$

is an ideal in $\mathfrak{o}$. (Dedekind, *Werke*, Vol. I, p. 126.)

Let $\mathfrak{p}$ be any prime ideal of $\Re(\theta)$ of which p is an element, and write

$$\mathfrak{o}p = \mathfrak{p}^e\mathfrak{q},$$

e being the highest power to which the ideal $\mathfrak{p}$ enters as a factor of p, so that $\mathfrak{q}$ is *not* divisible by $\mathfrak{p}$.

Suppose next that $F(x)$ is factored into its irreducible divisors (mod. p). Since the product of these divisors for $x=\theta$ is divisible by p, one of them is divisible by $\mathfrak{p}$. Let $P(x)$ be this factor of degree m, and suppose that (mod. p) the factor $P(x)$ enters $F(x)$ to the degree g, so that

$$F(x)\equiv P(x)^g\Pi(x) \text{ (mod. } p), \tag{1}$$

where $\Pi(x)$, modulo p, is not divisible by $P(x)$.

Observe next that every integer in $\mathfrak{o}_1$, and that is, every expression of the form $\varphi(\theta)$ above is congruent (mod. $\mathfrak{p}$) to one and only one expression

$$a_0+a_1\theta+\cdots+a_{m-1}\theta^{m-1},$$

in which the a's are rational integers including zero.

Since the a's may go through all values $0, 1, \cdots, p-1$, it is seen that *there are p^m incongruent integers in $\mathfrak{o}_1$, modulo $\mathfrak{p}$.*

If f is the degree of $\mathfrak{p}$, the number of such integers in $\mathfrak{o}$ is p^f, and that is,

$$(\mathfrak{o}, \mathfrak{p})=p^f=N(\mathfrak{p}).$$

The following theorem is fundamental in the further developments: THEOREM. *The necessary and sufficient conditions that the ideal $\mathfrak{f}$ be not divisible by $\mathfrak{p}$ are (1) that $m=f$ and (2) that $\mathfrak{p}$ be the greatest common ideal divisor of the two principal ideals $\mathfrak{o}p$ and $\mathfrak{o}P(\theta)$; and that is,*

$$\mathfrak{p}=(p, P(\theta)).$$

I. To prove that these two conditions given above are *necessary*, we must with Dedekind (Dirichlet-Dedekind, *Zahlentheorie*, p. 590) introduce the notion of the ring-leader of the order-modul $\mathfrak{o}_1$ which is denoted by $\mathfrak{f}$, where $\mathfrak{f}=\frac{\mathfrak{o}_1}{\mathfrak{o}}$. It follows that $\mathfrak{f}$ is the totality of integers γ, say,

for which

$$\mathfrak{o}\mathfrak{f} > \mathfrak{o}_1.$$

Since

$$\mathfrak{o}\mathfrak{f}\mathfrak{o} > \mathfrak{o}_1,$$

it is seen that the integers of $\mathfrak{f}\mathfrak{o}$ are included among the integers of $\mathfrak{f}$ and consequently

$$\mathfrak{o}\mathfrak{f} > \mathfrak{f}.$$

Since

$$[1] > \mathfrak{o},$$

we also have

$$\mathfrak{f} > \mathfrak{o}\mathfrak{f};$$

and therefore

$$\mathfrak{o}\mathfrak{f} = \mathfrak{f}.$$

Hence $\mathfrak{f}$ is an ideal of the given realm.

Further, since

$$\mathfrak{o}\mathfrak{f} > \mathfrak{o}_1 \quad \text{and} \quad \mathfrak{f} > \mathfrak{o}\mathfrak{f},$$

we observe that

$$\mathfrak{f} > \mathfrak{o}_1.$$

It is also true that every realm ideal $\mathfrak{i}$ which is contained in $\mathfrak{o}_1$ is also divisible by $\mathfrak{f}$. For,

$$\mathfrak{o}\mathfrak{i} > \mathfrak{o}_1,$$

and consequently the integers of $\mathfrak{o}\mathfrak{i}$ are among the γ's above. Since $\mathfrak{o}_1 > \mathfrak{o}$, it follows that $\mathfrak{o}\mathfrak{o}_1 > \mathfrak{o}\mathfrak{o}$ or $\mathfrak{o}\mathfrak{o}_1 > \mathfrak{o}$. We further have $[1] > \mathfrak{o}_1$, so that

$$\mathfrak{o}[1] > \mathfrak{o}\mathfrak{o}_1, \quad \text{or} \quad \mathfrak{o} > \mathfrak{o}\mathfrak{o}_1.$$

It follows that

$$\mathfrak{o}\mathfrak{o}_1 = \mathfrak{o}.$$

If $\mathfrak{f}$ is relatively prime to $\mathfrak{p}$, then their greatest common divisor is

$$\mathfrak{f} + \mathfrak{p} = \mathfrak{o}.$$

Accordingly,

$$\mathfrak{o} = \mathfrak{f} + \mathfrak{p} > \mathfrak{o}_1 + \mathfrak{p} > \mathfrak{o},$$

or

$$\mathfrak{o} = \mathfrak{o}_1 + \mathfrak{p}.$$

It follows (Vol. I, Art. 137), since

$$(\mathfrak{o}_1, \mathfrak{p}) = (\mathfrak{o}_1 + \mathfrak{p}, \mathfrak{p}),$$

that

$$(\mathfrak{o}_1, \mathfrak{p}) = (\mathfrak{o}, \mathfrak{p}) \qquad \text{or} \qquad p^m = p^f,$$

with which is proved the first assertion, namely, that

$$m = f.$$

Further $\mathfrak{p}$ is a *common divisor* of $\mathfrak{o}p$ and $\mathfrak{o} = P(\theta)$, since

$$P(\theta) \equiv 0 \pmod{\mathfrak{p}}.$$

If $\mathfrak{f}$ is *not* divisible [1] by $\mathfrak{p}$, then $\mathfrak{f}\mathfrak{p}$ is *not* divisible by $\mathfrak{p}^2$, and consequently, there is an integer τ, say, in $\mathfrak{p}\mathfrak{f}$, which is divisible by $\mathfrak{p}$ and *not* by $\mathfrak{p}^2$.

Further, since

$$\mathfrak{f}\mathfrak{p} > \mathfrak{p} > \mathfrak{o}_1,$$

it is seen that τ is a rational integral function of θ with rational integral coefficients, say

$$\tau = \Phi(\theta).$$

And, due to the fact that

$$\tau = \Phi(\theta) \equiv 0 \pmod{\mathfrak{p}},$$

it follows from (Vol. I, Art. 195) that this congruence is of the same meaning as the congruence

$$\Phi(x) \equiv P(x)Q(x) \pmod{p},$$

where $Q(x)$ is an integral function with rational integral coefficients.

From this latter congruence it follows that $P(\theta)$ and p are not simultaneously divisible by $\mathfrak{p}^2$; otherwise $\Phi(\theta)$ would be divisible by $\mathfrak{p}^2$.

Suppose next that $\mathfrak{p}'$ is a prime ideal factor of $\mathfrak{q}$, and observe that the ideal $\mathfrak{f}\mathfrak{p}'$ is *not* divisible by $\mathfrak{p}$. On the other hand, since

$$\mathfrak{f}\mathfrak{p}' > \mathfrak{f} > \mathfrak{o}_1,$$

[1] Ö. Ore has an interesting discussion of *ring-leaders* in *Math. Ann.*, Vol. 96, pp. 332 ff.

it is seen that there is an integer σ in $\mathfrak{f}\mathfrak{p}'$ which, like τ is of the form $\sigma = \Phi_1(\theta)$, where Φ_1 is a rational integral function of θ with rational integral coefficients.

Since, however,

$$\sigma = \Phi_1(\theta) \not\equiv 0 \pmod{\mathfrak{p}},$$

it follows (mod. p) that $\Phi_1(x)$ and $P(x)$ are relatively prime, and accordingly, two integral functions with rational integral coefficients $\Psi(x)$ and $X(x)$ may be found such that

$$P(x)\Psi(x) + \Phi_1(x)X(x) \equiv 1 \pmod{p}.$$

Writing $x = \theta$ in this congruence, and since

$$\Phi_1(\theta) \equiv 0 \pmod{\mathfrak{p}'},$$

we have

$$P(\theta)\Psi(\theta) \equiv 1 \pmod{\mathfrak{p}'}.$$

From this it is seen that $P(\theta)$ is *not* divisible by $\mathfrak{p}'$.

With this it is proved, if $\mathfrak{f}$ is *not* divisible by $\mathfrak{p}$, that the principal ideals $\mathfrak{o}p$ and $\mathfrak{o}P(\theta)$ are divisible by $\mathfrak{p}$ but not by $\mathfrak{p}^2$ nor by $\mathfrak{p}'$, where $\mathfrak{p}'$ is any other ideal divisor of p; and that is

$$\mathfrak{p} = (p, P(\theta)), \tag{2}$$

as was to be proved.

II. It may be shown next that the above two conditions are *sufficient*. For, if they are satisfied, the function $P(x)$ is (mod. p) a prime function of the same degree as the prime ideal $\mathfrak{p}$ and θ is a root of the congruence

$$P(x) \equiv 0 \pmod{\mathfrak{p}}, \qquad \text{where} \qquad \mathfrak{o}p = \mathfrak{p}^e q.$$

Due to the two assumptions, it is seen that θ, when $e > 1$, has the characteristic properties of those of the integer ρ of Arts. 63 and 64; and in particular, that $P(\theta)$, while divisible by $\mathfrak{p}$ is not divisible by $\mathfrak{p}^2$; and accordingly, loc. cit., every integer γ of $\mathfrak{o}$ is congruent (mod. $\mathfrak{p}^e$) to an integral function of θ; and that is, to an integer of $\mathfrak{o}_1$.

This result is also true when $e=1$; for, (Art. 62) every integer γ of $\mathfrak{o}$ may be expressed in the form

$$\gamma \equiv a_0 + a_1\theta + \cdots + a_{f-1}\theta^{f-1} \pmod{\mathfrak{p}}.$$

Hence, in all cases ω denoting an integer in $\mathfrak{o}_1$, we have

$$\gamma \equiv \omega \pmod{\mathfrak{p}^e}. \tag{3}$$

From formula (1) it is seen for $x=\theta$, that

$$P(\theta)^g \Pi(\theta) \equiv 0 \pmod{p}.$$

Observe that the integer p in this congruence may be replaced by one of its divisors $\mathfrak{q}$. Since $P(\theta)$ is not divisible by $\mathfrak{q}$, it follows, due to formula (1) above, that $\Pi(\theta)$ is divisible by $\mathfrak{q}$, but *not* by $\mathfrak{p}$, as $\Pi(x)$, modulo p, is not divisible by $P(x)$. Due to formula (3), it is seen that $\gamma-\omega$ is divisible by $\mathfrak{p}^2$, and accordingly, $(\gamma-\omega)\Pi(\theta)$ is divisible by $\mathfrak{p}^e\mathfrak{q}$; and that is, by p.

It follows that

$$\gamma\Pi(\theta) = \omega\Pi(\theta) + p\gamma_1,$$

where γ_1 is an integer in $\mathfrak{o}$. Observe that in this equation both ω and $\Pi(\theta)$ are integers of $\mathfrak{o}_1$, and consequently, also their product, so that the above equation may be written in the form of a congruence

$$\gamma\Pi(\theta) \equiv p\gamma_1 \pmod{\mathfrak{o}_1}.$$

Since γ is an arbitrary integer of $\mathfrak{o}$, we may form in a similar manner a series of congruences

$$\begin{aligned}
\gamma_1\Pi(\theta) &\equiv p\gamma_2 \pmod{\mathfrak{o}_1},\\
\gamma_2\Pi(\theta) &\equiv p\gamma_3 \pmod{\mathfrak{o}_1},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
\gamma_{s-1}\Pi(\theta) &\equiv p\gamma_s \pmod{\mathfrak{o}_1}.
\end{aligned}$$

Since $\mathfrak{o}_1$ is an order-modul, it follows from (Vol. I, Art. 133) that these congruences may be multiplied together, thus giving

$$\gamma\Pi(\theta)^s \equiv \gamma_s p^s \pmod{\mathfrak{o}_1}. \tag{4}$$

In this expression s may be taken as the highest power of p that enters the index C of θ, so that

$$C = cp^s,$$

where c is *not* divisible by p. Defining κ by the relation

$$\kappa = c\Pi(\theta)^s, \tag{5}$$

it follows from (4) that

$$\gamma\kappa \equiv C\gamma_s \pmod{\mathfrak{o}_1}. \tag{6}$$

Next observe that the index C of any integer θ of $\mathfrak{o} = [\omega_1, \omega_2, \cdots, \omega_n]$ is the determinant of the n linear equations through which the powers of θ, and that is, 1, $\theta, \cdots, \theta^{n-1}$ are expressed through the basal elements of $\mathfrak{o}$. From these n relations it is seen that each of these basal elements multiplied by C, and therefore also every integer of $\mathfrak{o}$ multiplied by C, may be expressed linearly with rational integral coefficients in terms of the powers of θ. Accordingly, it follows from (6) that every multiple of κ, and that is, the ideal $\mathfrak{o}\kappa$ is contained in $\mathfrak{o}_1$. It was proved above that every ideal in $\mathfrak{o}_1$ was divisible by the ring-leader of that order-modul. If then $\mathfrak{f}$ were divisible by $\mathfrak{p}$, it would follow that $\mathfrak{o}\kappa$ was divisible by $\mathfrak{p}$, which, from (5) is *not* true. With this it is proved that $\mathfrak{f}$ is NOT *divisible* by $\mathfrak{p}$. (See also Dedekind's *Werke*, Vol. I, p. 388; and Noether, *Crelle*, Vol. 157, pp. 82 ff., where many references are given.)

ART. **105.** A consequence of the above theorem is the following: THEOREM. *Corresponding to every given prime ideal* $\mathfrak{p}$ *there exists an integer* θ, *which generates the fixed realm* Ω *of the nth degree, so that* $\Omega = \Re(\theta)$, *and such that* $\mathfrak{p}$ *does not divide the ring leader* $\mathfrak{f}$ *of the order-modul* $\mathfrak{o}_1 = [1, \theta, \cdots, \theta^{n-1}]$.

To prove this, let ρ be a number as defined in Arts. 64 and 65, so that

$$\mathfrak{p} = (p, P(\rho)).$$

Next, let ζ be any integer that generates Ω and let $F(x)=0$ be the irreducible equation which ζ satisfies. Form the different

$$(1) \qquad \partial(\zeta)=(\zeta-\zeta^{(1)})(\zeta-\zeta^{(2)})\cdots(\zeta-\zeta^{(n-1)})=F'(\zeta),$$

where $\zeta^{(1)}$, $\zeta^{(2)}$, $\cdots$, $\zeta^{(n-1)}$ are the conjugates of ζ. Observe that this different is (Vol. I, Art. 96) different from zero.

Define θ by the relation

$$(2) \qquad \theta=\rho+px\zeta,$$

where x is an arbitrary rational integer. Observe that θ is an integer and satisfies the congruence

$$P(\theta)\equiv P(\rho) \pmod{p}.$$

It follows that

$$\mathfrak{p}=(p,\ P(\theta)).$$

The function $P(x)$ is irreducible (mod. p) of the fth degree, and ρ is a root of the congruence

$$P(x)\equiv 0 \pmod{\mathfrak{p}}.$$

Due to (2) it is seen that also

$$P(\theta)\equiv 0 \pmod{\mathfrak{p}}.$$

If $\Phi(x)=0$ is the equation of the nth degree which θ satisfies, so that $\Phi(\theta)=0$, it follows also that

$$\Phi(\theta)\equiv 0 \pmod{\mathfrak{p}},$$

and further, $P(x)$ is an irreducible (mod. p) factor of $\Phi(x)$, since both these functions are satisfied (mod. $\mathfrak{p}$) by θ.

From (2) it is seen that

$$\theta-\theta^{(i)}=\rho-\rho^{(i)}+px(\zeta-\zeta^{(i)}) \quad (i=1, 2, \cdots, n-1);$$

and (Vol. I, Arts. 50 and 51) we may so choose the rational integer x that the differences $\theta-\theta^{(i)}$ are all different from zero, as was the case with the differences $\zeta-\zeta^{(i)}$. It follows that the different $\partial(\theta)$ is different from zero and also (Vol. I, Art. 61) that $\Phi(x)=0$ is an

irreducible equation, and that θ is an integer that generates the fixed realm Ω.

It is thus proved that there exists an integer θ for which the conditions of the theorem are satisfied and that therefore the given prime ideal $\mathfrak{p}$ does *not* divide the ring leader $\mathfrak{f}$ of the order-modul $\mathfrak{o}$, that corresponds to this integer.

Finally it may be observed that, whereas there exist realms in which the indices of all integers are divisible by a certain rational prime integer p, due to the theorem just proved, it never happens that a given prime ideal $\mathfrak{p}$ is a factor of all the corresponding ring leaders $\mathfrak{f}$.

ART. **106.** Let θ be an integer which generates the realm $\Re(\theta)$ and let

$$F(x)=x^n+c_1x^{n-1}+\cdots+c_{n-1}x+c_n=0$$

be the irreducible equation which θ satisfies, the c's being rational integers.

Writing

$$(1)\quad \frac{F(x)}{x-\theta}=\alpha_0+\alpha_1x+\alpha_2x^2+\cdots+\alpha_{n-2}x^{n-2}+\alpha_{n-1}x^{n-1},$$

it is seen that

$$\begin{aligned}
\alpha_{n-1}&=1,\\
\alpha_{n-2}&=c_1+\theta,\\
\alpha_{n-3}&=c_2+c_1\theta+\theta^2,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
\alpha_1&=c_{n-2}+c_{n-1}\theta+\cdots+c_1\theta^{n-3}+\theta^{n-2},\\
\alpha_0&=c_{n-1}+c_{n-2}\theta+\cdots+c_1\theta^{n-2}+\theta^{n-1}.
\end{aligned}$$

Observe further that these numbers all belong to the order-modul $\mathfrak{o}_1$, that corresponds to θ. Since the determinant of the above n expressions is 1, it is clear that

$$[\alpha_0,\ \alpha_1,\ \cdots,\ \alpha_{n-1}]=[1,\ \theta,\ \cdots,\ \theta^{n-1}]=\mathfrak{o}_1.$$

In Vol. I, Art. 44 it was proved that every number ζ of $\Re(\theta)$ may be expressed as a function $f(\theta)$ of the $(n-1)$st

degree with rational coefficients. Also observe that

$$\frac{f(x)}{F(x)}=\frac{A_0}{x-\theta}+\frac{A_1}{x-\theta^{(1)}}+\cdots+\frac{A_{n-1}}{x-\theta^{(n-1)}},$$

where $\theta^{(1)}, \cdots, \theta^{(n-1)}$ are the conjugates of θ and that is, roots of $F(x)=0$. It follows that

$$f(x)=\frac{f(\theta)}{F'(\theta)}\frac{F(x)}{x-\theta}+\frac{f(\theta^{(1)})}{F'(\theta^{(1)})}\frac{F(x)}{x-\theta^{(1)}}+\cdots+\frac{f(\theta^{(n-1)})}{F'(\theta^{(n-1)})}\frac{F(x)}{x-\theta^{(n-1)}},$$

and that is,

$$f(x)=S\left(\frac{f(\theta)}{F'(\theta)}\frac{F(x)}{x-\theta}\right),$$

or, from (1)

$$f(x)=\sum_{i=0}^{i=n-1}S\left(\frac{f(\theta)}{F'(\theta)}\alpha_i\right)x^i.$$

Writing $x=\theta$, we have

$$f(\theta)=\zeta=\sum_{i=0}^{i=n-1}S\left(\frac{\alpha_i\zeta}{\partial(\theta)}\right)\cdot\theta^i,$$

where the different $\partial(\theta)$ is written for $F'(\theta)$.
From this it is clear that the numbers (see Vol. I, Art. 171)

$$\frac{\alpha_0}{\partial(\theta)}, \frac{\alpha_1}{\partial(\theta)}, \cdots, \frac{\alpha_{n-1}}{\partial(\theta)}$$

are the complementary basis of the basal numbers

$$1, \theta, \cdots, \theta^{n-1},$$

or

$$\left[\frac{\alpha_0}{\partial(\theta)}, \frac{\alpha_1}{\partial(\theta)}, \cdots, \frac{\alpha_{n-1}}{\partial(\theta)}\right]=\mathfrak{o}_1',$$

and that is

$$[\alpha_0, \alpha_1, \cdots, \alpha_{n-1}]=\partial(\theta)\mathfrak{o}_1',$$

where $\mathfrak{o}_1'$ and $\mathfrak{o}_1$ are complementary moduls.

We accordingly have

$$\mathfrak{o}_1=\partial(\theta)\mathfrak{o}_1'.$$

Since (Art. 104) the relation $\mathfrak{o}_1\mathfrak{o}=\mathfrak{o}$ is true of order-moduls, it follows that

$$\mathfrak{o}=\partial(\theta)\mathfrak{o}\mathfrak{o}_1',$$

and therefore also (Vol. I, Example 1, p. 279)

$$\mathfrak{o}' = (\partial(\theta)\mathfrak{o}\mathfrak{o}_1')' = \frac{(\mathfrak{o}\mathfrak{o}_1')'}{\partial(\theta)},$$

or

$$\mathfrak{o}'\partial(\theta) = (\mathfrak{o}\mathfrak{o}_1')' = \frac{(\mathfrak{o}_1')'}{\mathfrak{o}} = \frac{\mathfrak{o}_1}{\mathfrak{o}}.$$

And that is

$$\mathfrak{f} = \mathfrak{o}'\partial(\theta), \tag{i}$$

where $\mathfrak{o}'$ is the complementary modul of $\mathfrak{o}$.

On the other hand there exist among the basal elements ω_i of $\mathfrak{o}$ and the basal elements $\tilde{\omega}_i$ of the complementary modul (Vol. I, Art. 171) the relations

$$\omega_i = \sum_{k=1}^{k=n} S(\omega_i\omega_k)\tilde{\omega}_k \qquad (i=1, 2, \cdots, n). \tag{2}$$

Since the spurs $S(\omega_i\omega_k)$ are rational integers, it follows that

$$\mathfrak{o} > \mathfrak{o}'. \tag{3}$$

Observe that the determinant

$$|S(\omega_i\omega_k)| \qquad (i, k=1, 2, \cdots, n)$$

is (Vol. I, Art. 104) the basal invariant D of the realm. It follows through the solution of the equations (2), that each product $D\tilde{\omega}_k$ and therefore the product D multiplied by any integer in $\mathfrak{o}'$, is an integer in $\mathfrak{o}$, and that is,

$$D\mathfrak{o}' > \mathfrak{o}. \tag{4}$$

Next observe that $D\mathfrak{o}'$ is an ideal. For, since

$$(\mathfrak{o}\mathfrak{o}')' = \frac{\mathfrak{o}'}{\mathfrak{o}'} = \frac{\mathfrak{o}}{\mathfrak{o}},$$

and since for an order modul

$$\frac{\mathfrak{o}'\mathfrak{o}'}{\mathfrak{o}'} = \mathfrak{o}',$$

it follows that

$$\mathfrak{o}'\frac{\mathfrak{o}}{\mathfrak{o}} = \mathfrak{o}', \qquad \text{or} \qquad \mathfrak{o}\mathfrak{o}' = \mathfrak{o}'.$$

From (3) it is seen that

$$D\mathfrak{o} > D\mathfrak{o}'.$$

As the left hand ideal is divisible by the right hand ideal, it follows (Art. 14) that

$$D\mathfrak{o} = D\mathfrak{o}'\mathfrak{d},$$

where $\mathfrak{d}$ is an ideal. The ideal $\mathfrak{d}$ defined through the equation

$$\mathfrak{o} = \mathfrak{o}'\mathfrak{d} \qquad \text{(ii)}$$

was called by Dedekind [1] the *fundamental* or basal (*Grundideal*) ideal of the realm. (See also Art. 28.)

This ideal is of very great importance and is connected with the fundamental invariant D through the fact that the absolute value of the discriminant D is equal to the norm of $\mathfrak{d}$. For, from the relations (2) above, it follows (Vol. I, Art. 153) that

$$|D| = (\mathfrak{o}',\ \mathfrak{o}) = (\mathfrak{o}',\ \mathfrak{o}'\mathfrak{d}) = (\mathfrak{o},\ \mathfrak{d}),$$

or

$$|D| = N(\mathfrak{d}).$$

Multiplying the formula (i) above by $\mathfrak{d}$, it is seen that (cf. ii)

$$\mathfrak{d}\mathfrak{f} = \mathfrak{o}\partial(\theta). \qquad (5)$$

From this formula it follows that *the fundamental ideal* $\mathfrak{d}$ *is the greatest common divisor of the differents of all integers* γ *of the Gattung* $\mathfrak{G}$ *of the realm* $\Re(\theta)$. For, if these differents had a still greater divisor, it would follow that all the ring leaders $\mathfrak{f}$ of the associated order-moduls would have a common ideal prime divisor $\mathfrak{p}$; and as shown in the previous article, there exist integers of $\mathfrak{G}$ for which this is *not* the case.

ART. **107.** If in the fixed realm there exists an integer θ such that the n elements $1, \theta, \theta^2, \cdots, \theta^{n-1}$ form a basis of

[1] "Ueber die Discriminanten endlicher Körper," p. 38 of the paper as it appears in Vol. 29 of the *Gött. Abh.* See also Weber, *Algebra*, Vol. II, § 174.

all integers, then is

$$\mathfrak{o}_1 = \mathfrak{o}.$$

Since the complementary moduls must also be equal, it follows that

$$\mathfrak{o}_1' = \mathfrak{o}'.$$

Writing this in the formula

$$\mathfrak{o} = \partial(\theta)\mathfrak{o}\mathfrak{o}_1'$$

of the preceding article, it follows that

$$\mathfrak{o} = \partial(\theta)\mathfrak{o}'.$$

Further, since

$$\mathfrak{o} = \mathfrak{o}'\mathfrak{d},$$

it is seen that

$$\mathfrak{d}\mathfrak{o}' = \mathfrak{o}\partial(\theta)\mathfrak{o}',$$

or

$$\mathfrak{d} = \mathfrak{o}\partial(\theta),$$

a formula which determines for this special case the fundamental ideal.

ART. **108.** In general, let $\mathfrak{p}$ be an arbitrary prime ideal in a realm, which is generated by the integer θ, whose ring leader $\mathfrak{f}$ is not divisible by $\mathfrak{p}$. The necessary and sufficient conditions for this, as given in Art. 105, are

1°, $$\mathfrak{p} = (p, P(\theta))$$

and

2°, $P(x)$ is of degree f, which is also the degree of $\mathfrak{p}$. It may then be proved that the integers e and g of the two formulas (Art. 104)

$$\mathfrak{o}p = \mathfrak{p}^e\mathfrak{q} \qquad \text{and} \qquad F(x) \equiv P(x)^g \Pi(x) \pmod{p}$$

are equal, where $F(x) = 0$ is the irreducible equation of the nth degree that is satisfied by θ.

For, since $P(\theta)^g\Pi(\theta)$ is divisible by $\mathfrak{p}^e\mathfrak{q}$ and since

$$\Pi(\theta) \not\equiv 0 \pmod{\mathfrak{p}} \qquad \text{and} \qquad P(\theta) \not\equiv 0 \pmod{\mathfrak{p}^2},$$

it follows that

$$g \geqq e.$$

On the other hand, since

$$\Pi(\theta) \equiv 0 \pmod{\mathfrak{q}},$$

observe that

$$P(\theta)^e \Pi(\theta) = p\gamma,$$

where γ is an integer of $\mathfrak{o}$. Writing, as in Art. 104,

$$\kappa = c\Pi(\theta)^s,$$

where c is *not* divisible by p, and noting (loc. cit.) that $\gamma\kappa$ is an integer of $\mathfrak{o}_1$, it is seen that

$$cP(\theta)^e \Pi(\theta)^{s+1} = p\varphi(\theta),$$

where φ is an integral function with rational integral coefficients. Further, since θ satisfies the irreducible function $F(x)$, it follows from Vol. I, Art. 195 that

$$cP(x)^e \Pi(x)^{s+1} = p\varphi(x) + F(x)\Psi(x),$$

where $\Psi(x)$ is an integral function with rational integral coefficients. Writing for $F(x)$ its value from above, we have finally

$$cP(x)^e \Pi(x)^{s+1} \equiv P(x)^g \Pi(x)\Psi(x) \pmod{p}.$$

Since $\Pi(x)$ is not divisible by $P(x)$ it follows that $e \geqq g$, which with the previous result shows that $e = g$. Accordingly, we have

$$F(x) \equiv P(x)^e \Pi(x) \pmod{p}.$$

This formula differentiated gives

$$F'(x) \equiv P'(x)^{e-1} \Pi_1(x) \pmod{p},$$

where (see also Art. 92)

$$\Pi_1(x) = eP'(x)\Pi(x) + P(x)P'(x).$$

If e is *not* divisible by p, then $\Pi_1(x)$ is, modulo p, relatively prime to $P(x)$, this being true (Vol. I, Art. 41) of $P'(x)$ as also of $\Pi(x)$. Accordingly, from the formula

$$\partial(\theta) = F'(\theta) \equiv P'(\theta)^{e-1} \Pi_1(\theta) \pmod{\mathfrak{p}^e},$$

it is seen that $F'(\theta)$ is divisible by $\mathfrak{p}$ to the power $e-1$ and no higher. If however e *is* divisible by p, then is

$\Pi_1(x)$, modulo p, divisible by $P(x)$, and accordingly

$$\Pi_1(\theta) \equiv 0 \pmod{\mathfrak{p}}$$

and

$$\partial(\theta) = F'(\theta)$$

is divisible by $\mathfrak{p}$ to at least the eth power.

Returning to formula (5) of Art. 106, and with the assumption that $\mathfrak{f}$ is not divisible by $\mathfrak{p}$, we have the following fundamental theorem.

If $\mathfrak{p}$ is an arbitrary prime ideal and p the corresponding rational prime integer which is divisible by $\mathfrak{p}$ to the eth and no higher power, then the fundamental ideal $\mathfrak{d}$ contains $\mathfrak{p}$ as a factor to the power $e-1$ and no higher, unless e is divisible by p, in this case $\mathfrak{d}$ is factorable by $\mathfrak{p}$ to at least the eth power. (Dedekind, *Werke*, Vol. I, pp. 388 ff.)

From this theorem follows anew the theorem derived in Art. 92 and again in Arts. 31 and 77 regarding the factorization of the discriminant of the fixed realm D. For, since

$$|D| = N(\mathfrak{d}), \qquad \text{if} \qquad p = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r},$$

it follows that D is divisible by

$$p^{f_1(e_1-1)+f_2(e_2-1)+\cdots+f_r(e_r-1)}$$

and by no higher power of p unless one of the e's is divisible by p. If one of the e's is divisible by p, then p enters as a factor of D to a higher power than that just written.

Through the above theorem the connection between the fundamental invariant D and the fundamental ideal $\mathfrak{d}$ is put in a clear light except as to those singular ideal prime factors of p which occur as divisors of p to powers, which powers are divisible by p. Such integers p are called *singular*. Since they are divisors of one of the e's given above, and as

$$n = e_1f_1 + e_2f_2 + \cdots + e_rf_r,$$

it is seen that in any realm the number of such rational primes is very restricted. The last chapter of the present work is devoted to the discussion of these singular prime integers as divisors of the discriminants.

ART. 109. A remark found in Bachmann [1] is inserted here. Observe that

$$\begin{vmatrix} \omega_1, & \omega_2, & \cdots, & \omega_n \\ \omega_1^{(1)}, & \omega_2^{(1)}, & \cdots, & \omega_n^{(1)} \\ \cdots & \cdots & \cdots & \cdots \\ \omega_1^{(n-1)}, & \omega_2^{(n-1)}, & \cdots, & \omega_n^{(n-1)} \end{vmatrix} = \sqrt{D}.$$

Developing this determinant with respect to the first row, we have

$$\alpha_1\omega_1+\alpha_2\omega_2+\cdots+\alpha_n\omega_n=\sqrt{D},$$

where the subdeterminants α_i are algebraic integers of the fixed realm. If $\mathfrak{o}'$ is the complementary modul of $\mathfrak{o}$ and $\bar{\omega}_i$ are the elements of the complementary basis, it follows, as in Vol. I, Art. 173, due to the relation

$$\omega_1\bar{\omega}_1+\omega_2\bar{\omega}_2+\cdots+\omega_n\bar{\omega}_n=1$$

among the complementary elements, that

$$\bar{\omega}_i=\frac{\alpha_i}{\sqrt{D}}\,(i=1,\ 2,\ \cdots,\ n).$$

Observe that $D\bar{\omega}_i\bar{\omega}_k$ are integers in $\mathfrak{o}$, and accordingly that $D\mathfrak{o}'\mathfrak{o}'$ is contained in $\mathfrak{o}$. Since (Art. 104)

$$D\mathfrak{o}\mathfrak{o}'=D\mathfrak{o}' \qquad \text{and since} \qquad \mathfrak{o}D\mathfrak{o}'\mathfrak{o}'=D\mathfrak{o}\mathfrak{o}'\mathfrak{o}'=D\mathfrak{o}'\mathfrak{o}',$$

it follows that $D\mathfrak{o}'\mathfrak{o}'$ is an ideal. Denote this ideal by $\mathfrak{d}_1$.

The fundamental ideal $\mathfrak{d}$ was defined in Art. 106 by the formula $\mathfrak{o}=\mathfrak{d}\mathfrak{o}'$. Multiply this formula by $D\mathfrak{o}'$ and it is seen that

$$D\mathfrak{o}'=\mathfrak{d}\mathfrak{d}_1 \qquad \text{or} \qquad D\mathfrak{o}=\mathfrak{d}^2\mathfrak{d}_1,$$

and that is, *the fundamental invariant D is always divisible by the square of the fundamental ideal.*

[1] *Allgemeine Arithmetik*, etc., p. 318.

Passing to the norms, and noting (Art. 28) that

$$D = N(\mathfrak{d}),$$

it follows that

$$N(\mathfrak{d}_1) = D^{n-2}.$$

These results are due to Dedekind (*Werke* I, p. 382.)

EXAMPLE. Write

$$\mathfrak{d}_0 = \mathfrak{e}^{(1)}\mathfrak{e}^{(2)}\cdots\mathfrak{e}^{(n-1)},$$

where the $\mathfrak{e}$'s are the elements defined in Art. 77. Prove that

$$\mathfrak{d}_0 = \mathfrak{d},$$

where $\mathfrak{d}$ is the fundamental ideal; and that is, prove that the fundamental ideal is the content of the different of the fundamental form, or

$$\mathfrak{d} \simeq \partial(\xi),$$

where

$$\xi = u_1\omega_1 + u_2\omega_2 + \cdots + u_n\omega_n$$

is a root of the fundamental equation. (Art. 71.)

Remark. If

$$\mathfrak{o}_1 = [\tilde{\omega}_1, \tilde{\omega}_2, \cdots, \tilde{\omega}_n]$$

is an order-modul in

$$\mathfrak{o} = [\omega_1, \omega_2, \cdots, \omega_n],$$

then is

$$\tilde{\omega}_i = k_{i1}\omega_1 + k_{i2}\omega_2 + \cdots + k_{in}\omega_n \qquad (i = 1, 2, \cdots, n),$$

where the k's are rational integers.

Further, if

$$k = \pm |k_{ij}| \qquad \begin{pmatrix} i = 1, 2, \cdots, n \\ j = 1, 2, \cdots, n \end{pmatrix},$$

then $k\omega_1, k\omega_2, \cdots, k\omega_n$ are integers of $\mathfrak{o}_1$. It follows also that $k\omega$ is an integer of $\mathfrak{o}_1$, where ω is an integer of $\mathfrak{o}$. Hence Art. 104, as every ideal in $\mathfrak{o}_1$ is divisible by $\mathfrak{f}$, we have

$$k\mathfrak{o} > \mathfrak{f}.$$

In this connection see paper by Ö. Ore, *Math. Ann.*, Vol. 96, p. 347, where other references are found.

CHAPTER VII

ALGEBRAIC UNITS

I. The Dirichlet-Dedekind Theory

Art. **110.** Let $\Omega = \Re(\theta)$ be a definite realm of the nth degree, and let ϵ be a quantity of this realm such that both ϵ and $1/\epsilon$ are algebraic integers. That such quantities exist is proved in Arts. 120 and 132. It follows (Vol. I, Art. 89) that if 1 is divisible by ϵ, then $N(1)$ or 1 is divisible by $N(\epsilon)$; and consequently,

$$N(\epsilon) = \pm 1.$$

Reciprocally, it is clear that if $N(\epsilon) = \pm 1$, and if ϵ is an algebraic integer, then also is $1/\epsilon$ an algebraic integer. For, let the equation which ϵ satisfies be

$$\epsilon^n + a_1\epsilon^{n-1} + a_2\epsilon^{n-2} + \cdots + a_n = 0,$$

where $a_1, a_2, \cdots, a_n$ are rational integers and where

$$a_n = N(\epsilon) = \pm 1.$$

Further, since

$$1 + a_1\frac{1}{\epsilon} + a_2\left(\frac{1}{\epsilon}\right)^2 + \cdots \pm \left(\frac{1}{\epsilon}\right)^n = 0,$$

it is evident that $1/\epsilon$ is an algebraic integer.

Accordingly, the following definition of an algebraic unit is offered: *An algebraic integer ϵ is said to be a unit when its norm is equal to ± 1.* (Vol. I, Art. 90.) *And in this case $1/\epsilon$ is an algebraic integer, and in fact it is a unit.*

Art. **111.** In the present chapter a method will be given for presenting all the algebraic units of a fixed realm of rationality. It will be seen (Art. 129) that there

are always roots of unity in every realm, and these quantities are, of course, also algebraic units. If α is a root of unity, then all integral powers of α are roots of unity. If, further, α and β are two roots of unity, then the product of any power of α by any power of β is a root of unity. In general, if $\alpha, \beta, \gamma, \cdots$ are roots of unity, then also $\alpha^a\beta^b\gamma^c\cdots$, where $a, b, c, \cdots$ are rational integers, are roots of unity; and these roots, as is shown in algebra (Theory of Equations), may be expressed as integral powers of one single root of unity, say ϵ_0. If ϵ_0 is a primitive mth root of unity, then the following m powers

$$\epsilon_0^0, \epsilon_0^1, \epsilon_0^2, \cdots, \epsilon_0^{m-1}$$

are different from one another, while

$$\epsilon_0^m = \epsilon_0^0, \quad \epsilon_0^{m+1} = \epsilon_0^1, \quad \epsilon_0^{m+2} = \epsilon_0^2, \quad \cdots.$$

If the question is proposed: *How may all the algebraic units of a fixed realm be expressed*, it might be conjectured at once that they may be presented in the form

$$\epsilon_0^{m_0} \cdot \epsilon_1^{m_1} \cdot \epsilon_2^{m_2} \cdots,$$

where ϵ_0 is a definite primitive mth root of unity, and where $\epsilon_1, \epsilon_2, \cdots$ are other units of the realm, and $m_0, m_1, m_2, \cdots$ are rational integers (including zero). It will be seen that such a representation of all the units of Ω is possible, the presentation being formulated in the theorem of Dirichlet.[1]

THEOREM. *All the units of the realm Ω may be expressed through a finite number of them, say, $\epsilon_0, \epsilon_1, \epsilon_2, \cdots, \epsilon_{\nu-1}$ in such a way that from the product*

$$\epsilon_0^{m_0} \cdot \epsilon_1^{m_1} \cdot \epsilon_2^{m_2} \cdots \epsilon_{\nu-1}^{m_{\nu-1}}$$

every unit of the realm is had, and indeed, only once, when to m_0 are given the values $0, 1, 2, \cdots, m-1$, while $m_1, m_2,$

[1] Dirichlet, *Monatsber. der Berliner Akad. vom 30 Marz, 1846;* or *Werke*, Bd. 1, § 642.

$\ldots$, $m_{\nu-1}$ *are allowed to take all rational integral values* (*including zero*).

ART. **112.** The number ν, which appears in the theorem of the preceding article, has the following meaning. The realm Ω consists of all rational functions of a certain quantity ϑ with rational coefficients, where ϑ is the root of an irreducible equation $f(x)=0$ of the nth degree.

Let ϑ', ϑ'', $\cdots$, $\vartheta^{(n)}$ be the conjugate roots of the equation of which one root is ϑ itself. Further, let Ω_1, Ω_2, $\cdots$, Ω_n be conjugate realms of which one is Ω. For example, Ω_k consists of all rational functions of $\vartheta^{(k)}$ with rational coefficients. The realms Ω_1, Ω_2, $\cdots$, Ω_n need *not* be all different. If they are all equal, the realm Ω is called a *normal* realm (Vol. I, Art. 45).

If ϑ', say, is real, then all the quantities of Ω_1 are real, and Ω_1 is said to be a *real* realm.

If $\xi+i\eta$ is a root of $f(x)=0$, then also $\xi-i\eta$ is a root of this equation. Let

$$\vartheta'=\xi+i\eta \qquad \text{and} \qquad \vartheta''=\xi-i\eta,$$

so that Ω_1 consists of all quantities of the form $\varphi(\xi+i\eta)$, while Ω_2 consists of all quantities of the form $\varphi(\xi-i\eta)$, where φ denotes a rational function with rational coefficients. The realms Ω_1 and Ω_2 are called *conjugate* complex realms. It is evident that the number of pairs of conjugate complex realms is equal to the number of pairs of complex roots of the equation $f(x)=0$. If this number of pairs of conjugate roots of $f(x)=0$ is denoted by $n-\nu$, then, as will be seen later, ν is the number whose significance we are seeking.

The number of pairs of conjugate complex roots of $f(x)=0$ being $n-\nu$, the number of real roots of this equation is

$$n-2n+2\nu=2\nu-n;$$

and since

$$\nu = (2\nu - n) + (n - \nu),$$

it is seen that ν is equal to the sum of the number of real roots plus the number of pairs of complex roots; or, if two conjugate roots are counted as only one, the number of roots of $f(x) = 0$ is

$$(n - \nu) + (2\nu - n) = \nu.$$

ART. **113.** The proof of the theorem stated in Art. 111, as given by Dirichlet, is as follows. It may be noted first, if $\nu = 1$, that Ω is either the realm of rational quantities, or it is a quadratic realm with *negative* discriminant. In the absolute realm of rationality, $+1$ and -1 are the only units and they may both be expressed as powers of the primitive root -1. Let D denote the discriminant of the quadratic realms. If $D \neq -3$, and if $D \neq -4$, then $+1$ and -1 are the only units (Vol. I, Art. 99) in the quadratic realms with negative discriminant. If $D = -4$ then $+1, -1, +i, -i$ are the only units and they may be expressed as powers of i. When $D = -3$, there are (*loc. cit.*) six units which may be presented as powers of the sixth root of unity. This proves the theorem for the case $\nu = 1$.

Before considering the general case, it will be necessary first to prove the following *lemma.*

If x and s are two real positive quantities, and if $s > 1$, then always

$$(x+1)^s - x^s > 1.$$

For, differentiating this expression, it is seen that the derivative

$$s\{(x+1)^{s-1} - x^{s-1}\}$$

is positive, so that the function $(x+1)^s - x^s$ increases as x increases. As this function has the value 1 for $x = 0$, it has a greater value when $x > 0$.

If, then, we put $x=k$, where k is a positive integer, and if $s=\frac{n}{r}$, where n and r are two positive integers and $n>r$, it is seen that

$$(k+1)^{\frac{n}{r}}>k^{\frac{n}{r}}+1.$$

From this it is evident that between $k^{\frac{n}{r}}$ and $(k+1)^{\frac{n}{r}}$ there must be a positive integer, say m, such that

$$(k+1)^{\frac{n}{r}}>m\geqq k^{\frac{n}{r}}, \qquad \text{or} \qquad (k+1)^n>m^r\geqq k^n.$$

ART. 114. Suppose that the quantities $\omega_1, \omega_2, \cdots, \omega_n$ form a basis of all the integers of the fixed realm Ω of the nth degree, and let

$$0=[\omega_1, \omega_2, \cdots, \omega_n].$$

All integers of Ω are therefore of the form

$$\alpha=x_1\omega_1+x_2\omega_2+\cdots+x_n\omega_n,$$

where the x's are rational integers.

Let the conjugate quantities of ω_ν be $\omega_\nu', \omega_\nu'', \cdots, \omega_\nu^{(n)}$, while the conjugate quantities to α are denoted by $\alpha', \alpha'', \cdots, \alpha^{(n)}$. We thus have the n equations

$$\alpha^{(s)}=x_1\omega_1^{(s)}+x_2\omega_2^{(s)}+\cdots+x_n\omega_n^{(s)} \quad (s=1, 2, \cdots, n).$$

It follows that

$$|\alpha^{(s)}|\leqq|x_1||\omega_1^{(s)}|+|x_2||\omega_2^{(s)}|+\cdots+|x_n||\omega_n^{(s)}| \quad (s=1, 2, \cdots, n).$$

Suppose next that k is any positive integer, and choose the values

$$|x_1|, |x_2|, \cdots, |x_n|$$

all less than k. It is clear that

$$|\alpha^{(s)}|\leqq k\{|\omega_1^{(s)}|+|\omega_2^{(s)}|+\cdots+|\omega_n^{(s)}|\}.$$

The real quantities

$$|\omega_1^{(s)}|+|\omega_2^{(s)}|+\cdots+|\omega_n^{(s)}|$$

have n values for $s=1, 2, \cdots, n$. Let the greatest one of

these n values be c. It follows that

$$|\alpha^{(s)}| \leqq ck \qquad (s=1, 2, \cdots, n),$$

where c depends upon the realms, k being independent of them.

ART. **115.** As the thereom to be proved (Art. 111) has been shown to be true for $\nu = 1$, it remains only to prove it for ν greater than unity. The realms $\Omega_1, \Omega_2, \cdots, \Omega_n$ may, under this hypothesis, be distributed into two groups, where there is at least *one* realm in either group; and further, any two conjugate complex realms are always put in the same group. Suppose further that the selection has been made that the first group consists of the realms $\Omega_1, \Omega_2, \cdots, \Omega_r$, while the second group contains the realms $\Omega_{r+1}, \Omega_{r+2}, \cdots, \Omega_n$.

In the expression

$$\alpha = x_1\omega_1 + x_2\omega_2 + \cdots + x_n\omega_n,$$

let α be decomposed into its real and imaginary components. If then

$$\begin{aligned}
\omega_1 &= w_{11} + iw_{21},\\
\omega_2 &= w_{12} + iw_{22},\\
\omega_3 &= w_{13} + iw_{23},\\
&\cdots\cdots\cdots\cdots\\
\omega_n &= w_{1n} + iw_{2n};
\end{aligned}$$

and if

$$\alpha = y_1 + iy_2,$$

it is clear that

$$\begin{aligned}
y_1 &= w_{11}x_1 + w_{12}x_2 + \cdots + w_{1n}x_n,\\
y_2 &= w_{21}x_1 + w_{22}x_2 + \cdots + w_{2n}x_n.
\end{aligned}$$

When this has been done for all the real and complex quantities that are conjugate to α, there appear the additional linear forms, say

$$\begin{aligned}
y_3 &= w_{31}x_1 + w_{32}x_2 + \cdots + w_{3n}x_n,\\
y_4 &= w_{41}x_1 + w_{42}x_2 + \cdots + w_{4n}x_n,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
y_n &= w_{n1}x_1 + w_{n2}x_2 + \cdots + w_{nn}x_n.
\end{aligned}$$

If Ω_a is a real realm, let

$$\omega_r^{(a)} = w_{ar};$$

while, if Ω_a and Ω_b are conjugate complex realms, let

$$\omega_r^{(a)} = w_{ar} + iw_{br} \quad \text{and} \quad \omega_r^{(b)} = w_{ar} - iw_{br} \quad (r = 1, 2, \cdots, n).$$

Hence, for a real realm Ω_a it follows that

$$|w_{a1}| + |w_{a2}| + \cdots |w_{an}| = |\omega_1^{(a)}| + |\omega_2^{(a)}| + \cdots + |\omega_n^{(a)}|.$$

In Art. 114 it appeared that c is the greatest value which the sum

$$|\omega_1^{(a)}| + |\omega_2^{(a)}| + \cdots + |\omega_n^{(a)}|$$

can have for $a = 1, 2, \cdots, n$. It follows that

$$|w_{a1}| + |w_{a2}| + \cdots + |w_{an}| \leqq c.$$

This is also true if Ω_a is a complex realm. For, if Ω_b is the conjugate complex realm, it is seen that

$$|w_{a1}| + |w_{a2}| + \cdots + |w_{an}|$$

$$= \sum_{r=1}^{r=n} |w_{ar}| \leqq \sum_{r=1}^{r=n} \sqrt{w_{ar}^2 + w_{br}^2} \leqq \sum |\omega_r^{(a)}| \leqq c \quad (a = 1, 2, \cdots, n).$$

ART. 116. In the n linear forms for the y's of the preceding article, let the variables $x_1, x_2, \cdots, x_n$ take only the values $0, 1, 2, \cdots, k$. We then have

$$\begin{aligned} |y_s| &\leqq |w_{s1}| x_1 + |w_{s2}| x_2 + \cdots + |w_{sn}| x_n \\ &\leqq k[\,|w_{s1}| + |w_{s2}| + \cdots + |w_{sn}|\,]; \end{aligned}$$

or

$$|y_s| \leqq ck \qquad (s = 1, 2, \cdots, n).$$

It is evident, when the variables $x_1, x_2, \cdots, x_n$ take the values $0, 1, 2, \cdots, k$, that the values of the linear forms for $y_1, y_2, \cdots, y_n$ lie between $-ck$ and $+ck$.

Determine next the positive integer m (Art. 113) such that

$$(k+1)^n > m^r \geqq k^n,$$

where r is the number of realms that belong to the first group. Divide the interval from $-ck$ to $+ck$, whose

expanse is $2ck$, into m equal parts, where the length of each of the intervals is $\frac{2ck}{m}=d$, say. To the variables x_1, $x_2, \cdots, x_n$ give any of the values $0, 1, 2, \cdots, k$ and consider the first r linear forms $y_1, y_2, \cdots, y_r$, which belong to the realm of the first group $\Omega_1, \Omega_2, \cdots, \Omega_r$. Since x_1 may take any of the values $0, 1, \cdots, k$, as may also x_2, $x_3, \cdots, x_n$, there are $(k+1)^n$ systems of values, which each of the forms $y_1, y_2, \cdots, y_r$ may take. These y's must lie in the m intervals above, say y_1 in the s_1-interval, y_2 in the s_2-interval, $\cdots$, y_r in the s_r-interval. Since each of the r numbers $s_1, s_2, \cdots, s_r$ may have the values $1, 2, \cdots, m$, there are in all m^r different arrangements possible of the y's that are r in number.

Since

$$(k+1)^n > m^r,$$

we must have at least

$$(k+1)^n = l+1,$$

where

$$l = m^r.$$

As all possible different arrangements that may be had is l, it is seen that for two different systems of values of the x's, the y's fall within the same intervals.

Suppose these two systems are

$$x_i = a_i \quad \text{and} \quad x_i = b_i \qquad (i=1, 2, \cdots, n),$$

and that the corresponding values of the y's are

$$y_j = u_j \quad \text{and} \quad y_j = v_j \qquad (j=1, 2, \cdots, r).$$

It follows that

$$|u_j - v_j| < d \qquad (j=1, 2, \cdots, r),$$

while the differences

$$a_i - b_i \leqq k$$

are *not* all zero. We had

$$d = \frac{2ck}{m} \quad \text{and} \quad m^r \geqq k^n,$$

so that

$$m \leqq k^{\frac{n}{r}}.$$

It follows that

$$d \leqq \frac{2ck}{k^{\frac{n}{r}}} \leqq \frac{2c}{k^{\frac{n}{r}-1}}.$$

ART. 117. Observe that

$$\alpha = x_1\omega_1 + x_2\omega_2 + \cdots + x_n\omega_n$$

is an arbitrary integer in Ω. If $\Omega_{s'}$ and Ω_s are two conjugate complex realms, write

$$\alpha^{(s')} = \bar{y}_{s'} + i\bar{y}_s,$$

$$\alpha^{(s)} = \bar{y}_{s'} - i\bar{y}_s;$$

while, if Ω_s is a real realm, put

$$\alpha^{(s)} = \bar{y}_s.$$

It follows at once from the preceding article that to the variables $x_1, x_2, \cdots, x_n$ may be given such values

$$a_1 - b_1,\ a_2 - b_2,\ \cdots,\ a_n - b_n$$

that the corresponding linear forms

$$\bar{y}_j = u_j - v_j \qquad (j = 1, 2, \cdots, r),$$

which belong to the variables $\Omega_1, \Omega_2, \cdots, \Omega_r$, are all less than d. It is thus seen in the case of the conjugate complex realms that

$$|\alpha^{(s)}| = \sqrt{\bar{y}_{s'}^2 + \bar{y}_{s'}^2} \leqq \sqrt{d^2 + d^2} \leqq d\sqrt{2} \leqq \frac{2c}{k^{\frac{n}{r}-1}}\sqrt{2} < \frac{3c}{k^{\frac{n}{r}-1}}.$$

If Ω_s is a real realm, it was proved above that

$$|\alpha^{(s)}| \leqq \frac{2c}{k^{\frac{n}{r}-1}}.$$

It has thus been shown that an integer α may always be found in the realm Ω, such that the first r quantities $\alpha', \alpha'', \cdots, \alpha^{(r)}$ that are conjugate to α (including α) and

which belong respectively to the realms $\Omega_1, \Omega_2, \cdots, \Omega_r$, are in absolute value less than $\dfrac{3c}{k^{\frac{n}{r}-1}}$.

Consider next the quantities

$$\alpha^{(r+1)}, \alpha^{(r+2)}, \cdots, \alpha^{(n)},$$

which belong to the realms $\Omega_{r+1}, \Omega_{r+2}, \cdots, \Omega_n$. In Art. 114 it was seen that, if to the variables $x_1, x_2, \cdots, x_n$ were given integral values less than k,

$$|\alpha^{(r+l)}| \leqq ck < 3ck \qquad (l=1, 2, \cdots, n-r).$$

ART. 118. It has thus been proved that there exists an integer α different from zero in the realm Ω, which has the following properties:

(1) the coordinates of α lie between 0 and k, where k is an arbitrary positive integer;

(2) it is possible to distribute the realms into two groups such that the quantities which are conjugate to α, namely, $\alpha', \alpha'', \cdots, \alpha^{(n)}$ fall into two groups

$$\alpha', \alpha'', \cdots, \alpha^{(r)} \quad \text{and} \quad \alpha^{(r+1)}, \alpha^{(r+2)}, \cdots, \alpha^{(n)},$$

where the quantities of the first group are in absolute value less than

$$\frac{3c}{k^{\frac{n}{r}-1}},$$

while the quantities of the second group, are all less than $3ck$, the constant c depending upon the nature of the realm.

From these properties of the integer α it is clear that

$$\prod_{l=1}^{l=r} |\alpha^{(l)}| < \left(\frac{3c}{k^{\frac{n}{r}-1}}\right)^r < \frac{(3c)^r}{k^{n-r}}$$

and

$$\prod_{l=r+1}^{l=n} |\alpha^{(l)}| < (3ck)^{n-r}.$$

It is evident that

$$|N(\alpha)| = \prod_{l=1}^{l=n} |\alpha^{(l)}| < (3c)^n.$$

Further, since α is an algebraic integer, that is not a unit, it follows that

$$|N(\alpha)| \geqq 1.$$

ART. 119. Let β be one of the numbers $\alpha^{(r+1)}, \alpha^{(r+2)}, \cdots, \alpha^{(n)}$. The product of the remaining $n-r-1$ of these numbers is less than

$$(3ck)^{n-r-1},$$

so that

$$|N(\alpha)| < \frac{(3c)^r}{k^{n-r}} \; |\beta| (3ck)^{n-r-1} < |\beta| \frac{(3c)^{n-1}}{k};$$

or

$$|\beta| > |N(\alpha)| \frac{k}{(3c)^{n-1}}.$$

Since $|N(\alpha)| \geqq 1$, it follows that

$$|\beta| > \frac{k}{(3c)^{n-1}}.$$

From this it is seen that the quantities $\alpha', \alpha'', \cdots, \alpha^{(n)}$ which are conjugate to α, including α, may be distributed into two groups

$$\alpha', \alpha'', \cdots, \alpha^{(r)} \qquad \text{and} \qquad \alpha^{(r+1)}, \alpha^{(r+2)}, \cdots, \alpha^{(n)}$$

in such a way that each quantity belonging to the first group is in absolute value less than $\frac{3c}{k^{\frac{n}{r}-1}}$, while each quantity of the second group is in absolute value greater than $\frac{k}{(3c)^{n-1}}$. If k is taken sufficiently large, the quantity $\frac{3c}{k^{\frac{n}{r}-1}}$ may be made arbitrarily small, since $n > r$, while at the same time $\frac{k}{(3c)^{n-1}}$ is arbitrarily large. If, then, A is

an arbitrarily small quantity, while B is an arbitrarily large quantity, it is evident that k may be taken so large that

$$\frac{k}{(3c)^{n-1}} > B \tag{1}$$

and

$$\frac{3c}{k^{\frac{n}{r}-1}} < A. \tag{2}$$

If, further, we put

$$(3c)^n = C,$$

then, from above

$$|N(\alpha)| < C.$$

Observe that C is independent of A, B and r.

Accordingly, it has been proved that there exists in the realm Ω an algebraic integer α different from zero, which has the properties that

$$|N(\alpha)| < C,$$

where C is definitely determined; and that the conjugate quantities

$$\alpha', \alpha'', \cdots, \alpha^{(n)}$$

may be distributed into groups

$$\alpha', \alpha'', \cdots, \alpha^{(r)} \qquad \text{and} \qquad \alpha^{(r+1)}, \alpha^{(r+2)}, \cdots, \alpha^{(n)},$$

such that every quantity of the first group is less than A, while every quantity of the second group is greater than B, in absolute value, the quantities A and B being perfectly arbitrary except that $A < B$.

ART. 120. Having determined a quantity α which satisfies the conditions of the preceding article, denote by A_1 the smallest of the quantities

$$|\alpha'|, |\alpha''|, \cdots, |\alpha^{(r)}|,$$

and let B_1 be the largest of the quantities

$$|\alpha^{(r+1)}|, |\alpha^{(r+2)}|, \cdots, |\alpha^{(n)}|.$$

It is clear that

$$A_1 < A \qquad \text{and} \qquad B_1 > B.$$

As seen above, we may again determine an integer α_1 belonging to Ω where

$$|N(\alpha_1)| < C,$$

and such that $\alpha_1', \alpha_1'', \cdots, \alpha_1^{(r)}$ in absolute value are less than A_1, while $\alpha_1^{(r+1)}, \alpha_1^{(r+2)}, \cdots, \alpha_1^{(n)}$ are in absolute value greater than B_1. The quantity α_1 is not identical with α, since A_1 is the smallest of the quantities

$$|\alpha'|, |\alpha''|, \cdots, |\alpha^{(r)}|,$$

while all the quantities

$$|\alpha_1'|, |\alpha_1''|, \cdots, |\alpha_1^{(r)}|$$

are less than A_1.

Continuing, let A_2 equal the smallest of the quantities

$$|\alpha_1'|, |\alpha_1''|, \cdots, |\alpha_1^{(r)}|;$$

and let B_2 equal the largest of the quantities

$$|\alpha_1^{(r+1)}|, |\alpha_1^{(r+2)}|, \cdots, |\alpha_1^{(n)}|.$$

It is then possible to determine another integer α_2 such that

$$|N(\alpha_2)| < C,$$

and such that

$$|\alpha_2'|, |\alpha_2''|, \cdots, |\alpha_2^{(r)}|$$

are less than A_2, while

$$|\alpha_2^{(r+1)}|, |\alpha_2^{(r+2)}|, \cdots, |\alpha_2^{(n)}|$$

are greater than B_2, and

$$\alpha_2 \neq \alpha_1.$$

Continuing this process we may derive an infinite number of algebraic integers $\alpha, \alpha_1, \alpha_2, \cdots$, that are different from zero and which belong to Ω. They all have the property that their norms are less than a fixed quantity C. There are, however, only a finite number of rational integers which are less than C, so that the

number of different norms less than C is finite. Hence, there must be in Ω an infinite number of integers which have the same norm; and that is, there is an integer $g \leqq C$, which occurs infinitely often as a norm.

It is possible to distribute all these integers, whose norms are equal to g, into different classes (mod. g); and as each such integer has the form $x_1\omega_1+x_2\omega_2+\cdots+x_n\omega_n$; and since each x may take values

$$0, 1, 2, \cdots, g-1,$$

there are evidently g^n such classes. One of these classes must contain an infinite number of integers; and that is, there must be an infinite number of integers, which are congruent (mod. g) and whose norms are equal to g. Let α and β be two such integers, so that

$$\alpha \equiv \beta \pmod{g} \tag{1}$$

and

$$N(\alpha) = N(\beta) = g. \tag{2}$$

Since $N(\alpha)=g$, it follows (Vol. I, Art. 90) that g is divisible by α; and since $N(\beta)=g$, it is seen also that g is divisible by β.

Further, owing to (1), $\alpha-\beta$ is divisible by g; and since g is divisible by α, it follows that $\alpha-\beta$ is divisible by α, and consequently β is divisible by α. Similarly, it is seen that α is divisible by β. It follows that $\frac{\alpha}{\beta}$ and $\frac{\beta}{\alpha}$ are algebraic units. Observe that

$$N\left(\frac{\alpha}{\beta}\right) = \frac{N(\alpha)}{N(\beta)} = 1.$$

It is evident from above that it is possible to choose the numbers α and β, such that α', α'', $\cdots$, $\alpha^{(r)}$ are in absolute value greater than

$$|\beta'|, |\beta''|, \cdots, |\beta^{(r)}|,$$

while all the quantities

$$|\alpha^{(r+1)}|,\ |\alpha^{(r+2)}|,\ \cdots,|\alpha^{(n)}|$$

are less than

$$|\beta^{(r+1)}|,\ |\beta^{(r+2)}|,\ \cdots,|\beta^{(n)}|.$$

It follows that the quotients

$$\left|\frac{\alpha'}{\beta'}\right|,\ \left|\frac{\alpha''}{\beta''}\right|,\ \cdots,\ \left|\frac{\alpha^{(r)}}{\beta^{(r)}}\right|$$

are all greater than 1, while the quotients

$$\left|\frac{\alpha^{(r+1)}}{\beta^{(r+1)}}\right|,\ \left|\frac{\alpha^{(r+2)}}{\beta^{(r+2)}}\right|,\ \cdots,\ \left|\frac{\alpha^{(n)}}{\beta^{(n)}}\right|$$

are all less than 1. Writing

$$\frac{\alpha}{\beta}=\epsilon,$$

we have

$$\frac{\alpha'}{\beta'}=\epsilon',\ \cdots,\ \frac{\alpha^{(n)}}{\beta^{(n)}}=\epsilon^{(n)}.$$

It is thus shown that in the realm Ω there is a unit ϵ, such that the conjugate units may be distributed into two groups

$$\epsilon',\ \epsilon'',\ \cdots,\ \epsilon^{(r)} \qquad \text{and} \qquad \epsilon^{(r+1)},\ \epsilon^{(r+2)},\ \cdots,\ \epsilon^{(n)},$$

and that the units of the first group are in absolute value greater than 1, while the units of the second group are in absolute value less than 1.

ART. 121. Consider next the logarithms of the units of the preceding article. If z is any complex quantity, say

$$z=x+iy,$$

write

$$x=R\cos\varphi, \qquad y=R\sin\varphi,$$

so that

$$z=R(\cos\varphi+i\sin\varphi)=Re^{i\varphi}=Re^{i\varphi+2ki\pi}.$$

It follows that

$$\log z=\log R+i\varphi+2ki\pi.$$

From this it is seen that the real part of $\log z$ is equal to the real quantity R or to $\log |z|$, a quantity which is denoted by lz. From the theorem of Art. 120, end, it is seen that

$$l\epsilon', l\epsilon'', \cdots, l\epsilon^{(r)}$$

are all greater than zero, while

$$l\epsilon^{(r+1)}, l\epsilon^{(r+2)}, \cdots, l\epsilon^{(n)}$$

are all less than zero. If of the n realms that are conjugate to Ω we omit one of every pair of conjugate realms, there are ν realms (Art. 112) which are distributed into two groups. In a corresponding manner, of the n quantities

$$l\epsilon', l\epsilon'', \cdots, l\epsilon^{(n)}$$

there remain ν, provided one of every pair of conjugate complex units is omitted.

Suppose that η is any arbitrary algebraic integer of the realm Ω, and let $\eta', \eta'', \cdots, \eta^{(n)}$ be conjugates of the quantities η, so that

$$N(\eta) = \eta' \cdot \eta'' \cdots \eta^{(n)},$$

or

$$|N(\eta)| = |\eta'| \cdot |\eta''| \cdots |\eta^{(n)}|.$$

Let s and t be any two of the numbers $1, 2, \cdots, n$ and define a number c_s through the following conditions:

$$c_s = 1, \text{ if } \eta^{(s)} \text{ is real,}$$
$$\text{while } c_s = 2, \text{ if } \eta^{(s)} \text{ is complex.}$$

If then $\eta^{(s)}$ and $\eta^{(t)}$ are conjugate complex quantities, we have

$$|\eta^{(s)}| \cdot |\eta^{(t)}| = |\eta^{(s)}|^2.$$

It follows that

$$|N(\eta)| = |\eta'|^{c_1} \cdot |\eta''|^{c_2} \cdots |\eta^{(\nu)}|^{c_\nu};$$

and consequently

$$l|N(\eta)| = c_1 l\eta' + c_2 l\eta'' + \cdots + c_\nu l\eta^{(\nu)}.$$

Suppose next that $\epsilon_1, \epsilon_2, \cdots, \epsilon_\nu$ are ν arbitrary units of the realm Ω. It is evident, since

$$|N(\epsilon_1)| = 1 = |N(\epsilon_2)| = \cdots = |N(\epsilon_\nu)|,$$

that

$$lN(\epsilon_1) = 0 = lN(\epsilon_2) = \cdots = lN(\epsilon_\nu),$$

with the resulting ν linear homogeneous equations

$$\begin{aligned}
&c_1 l\epsilon_1' + c_2 l\epsilon_1'' + c_3 l\epsilon_1''' + \cdots + c_\nu l\epsilon_1^{(\nu)} = 0,\\
&c_1 l\epsilon_2' + c_2 l\epsilon_2'' + c_3 l\epsilon_2''' + \cdots + c_\nu l\epsilon_2^{(\nu)} = 0,\\
&\cdots + \cdots + \cdots + \cdots + \cdots\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&c_1 l\epsilon_\nu' + c_2 l\epsilon_\nu'' + c_3 l\epsilon_\nu''' + \cdots + c_\nu l\epsilon_\nu^{(\nu)} = 0.
\end{aligned}$$

As the quantities $c_1, c_2, \cdots, c_\nu$ are *not* equal to zero, the above system of homogeneous linear equations can exist only if the determinant of the νth degree is zero; and that is, if

$$|l\epsilon_r^{(s)}| = 0 \qquad (r, s = 1, 2, \cdots, \nu).$$

With this is proved the following theorem; *If* $\epsilon_1, \epsilon_2, \cdots, \epsilon_\nu$ *is a system of* ν *units belonging to* Ω, *then always*

$$\begin{vmatrix}
l\epsilon_1', & l\epsilon_1'', & \cdots, & l\epsilon_1^{(\nu)}\\
l\epsilon_2', & l\epsilon_2'', & \cdots, & l\epsilon_2^{(\nu)}\\
\cdot & \cdot & \cdot & \cdot\\
\cdot & \cdot & \cdot & \cdot\\
\cdot & \cdot & \cdot & \cdot\\
l\epsilon_\nu', & l\epsilon_\nu'', & \cdots, & l\epsilon_\nu^{(\nu)}
\end{vmatrix} = 0.$$

ART. 122. On the other hand, the following theorem may be proved: *If* μ *is any one of the numbers* 1, 2, $\cdots$, $\nu - 1$, *it is always possible to determine* μ *units* $\epsilon_1, \epsilon_2, \cdots, \epsilon_\mu$ *in the realm* Ω *such that the determinant of the* μ*th order*

$$|l\epsilon_r^{(s)}| \neq 0 \qquad (r, s = 1, 2, \cdots, \mu).$$

For, if $\mu = 1$, it has been proved that it is possible to choose a unit ϵ_1 such that

$$l\epsilon_1', l\epsilon_1'', \cdots, l\epsilon_1^{(r)}$$

are individually greater than zero, while

$$l\epsilon_1^{(r+1)}<0,\ l\epsilon_1^{(r+2)}<0,\ \cdots,\ l\epsilon_1^{(n)}<0.$$

If the distribution of the realms $\Omega_1, \Omega_2, \cdots, \Omega_n$ into two groups is such that the first group contains only the one realm Ω_1, where, in the case of a pair of complex realms only one is kept; while the second group contains all the other realms, then it follows at once that

$$l\epsilon_1'>0,$$

while

$$l\epsilon_1'',\ l\epsilon_1''',\ \cdots,\ l\epsilon_1^{(n)}$$

are all less than zero, so that the theorem is true for $\mu=1$.

Assuming the theorem to be true for $\mu-1$, it may be proved to be true for μ as follows: Suppose that we have determined $\mu-1$ units

$$\epsilon_1,\ \epsilon_2,\ \cdots,\ \epsilon_{\mu-1}$$

in the realm Ω, such that

$$D_{\mu-1}=\begin{vmatrix} l\epsilon_1', & l\epsilon_1'', & \cdots, & l\epsilon_1^{(\mu-1)} \\ l\epsilon_2', & l\epsilon_2'', & \cdots, & l\epsilon_2^{(\mu-1)} \\ \cdots & \cdots & \cdots & \cdots \\ l\epsilon_{\mu-1}', & l\epsilon_{\mu-1}'', & \cdots, & l\epsilon_{\mu-1}^{(\mu-1)} \end{vmatrix}$$

has a value different from zero. It may be assumed that $D_{\mu-1}$ is positive without limiting the generality of the problem. For, if

$$D_{\mu-1}<0,$$

it is only necessary to interchange two consecutive rows or columns in the determinant.

It may be proved next that a unit ϵ_μ may be so determined in Ω that the determinant

$$D_\mu=\begin{vmatrix} l\epsilon_1', & l\epsilon_1'', & \cdots, & l\epsilon_1^{(\mu-1)}, & l\epsilon_1^{(\mu)} \\ l\epsilon_2', & l\epsilon_2'', & \cdots, & l\epsilon_2^{(\mu-1)}, & l\epsilon_2^{(\mu)} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ l\epsilon_\mu', & l\epsilon_\mu'', & \cdots, & l\epsilon_\mu^{(\mu-1)}, & l\epsilon_\mu^{(\mu)} \end{vmatrix}$$

has a value different from zero. For, if this determinant

is developed with respect to the elements of the last row, it is seen that

$$(1) \qquad D_\mu = C_1 l\epsilon'_\mu + C_2 l\epsilon''_\mu + \cdots + C_{\mu-1} l\epsilon_\mu^{(\mu-1)} + D_{\mu-1} l\epsilon_\mu^{(\mu)},$$

where $C_1, C_2, \cdots, C_{\mu-1}$ are definite determinants of the $(\mu-1)$st order composed of $l\epsilon'_1, l\epsilon''_1, \cdots, l\epsilon_{\mu-1}^{(\mu-1)}$.

Make a distribution of the realms $\Omega_1, \Omega_2, \cdots, \Omega_\nu$ into two groups as follows: Take Ω_μ in the first group, while $\Omega_{\mu+1}, \Omega_{\mu+2}, \cdots, \Omega_\nu$ are taken in the second group. If further s is one of the numbers $1, 2, \cdots, \mu-1$, then Ω_s is taken in the first group if C_s is positive; but it is put in the second group if $C_s \leqq 0$.

Next determine a unit ϵ_μ in Ω, such that

$$l\epsilon'_\mu, \; l\epsilon''_\mu, \; \cdots, \; l\epsilon_\mu^{(\mu+1)}$$

fall within these respective realms. It follows that all the *summands* on the right hand side of the expression (1) are positive, and consequently also, D_μ has a positive value. Since the theorem is true for $\mu = 1$, it is true for $\mu = 2, 3, \cdots, \nu-1$.

Thus the following theorem is proved: *It is always possible to determine $\nu-1$ units, say, $\epsilon_1, \epsilon_2, \cdots, \epsilon_{\nu-1}$ of the realm Ω, such that the determinant of the $(\nu-1)$st order*

$$D_{\nu-1} = \begin{vmatrix} l\epsilon'_1, & l\epsilon''_1, & \cdots, & l\epsilon_1^{(\nu-1)} \\ l\epsilon'_2, & l\epsilon''_2, & \cdots, & l\epsilon_2^{(\nu-1)} \\ \cdots & \cdots & \cdots & \cdots \\ l\epsilon'_{\nu-1}, & l\epsilon''_{\nu-1}, & \cdots, & l\epsilon_{\nu-1}^{(\nu-1)} \end{vmatrix}$$

has a value different from zero, and this determinant may be taken positive.

Such a system of units $\epsilon_1, \epsilon_2, \cdots, \epsilon_{\nu-1}$ is called a *system of independent units.* The determinant $D_{\nu-1}$ is denoted by $L(\epsilon_1, \epsilon_2, \cdots, \epsilon_{\nu-1})$.

ART. 123. Let σ be an arbitrary quantity having the form

$$(1) \qquad \sigma = \epsilon_1^{m_1} \epsilon_2^{m_2} \cdots \epsilon_{\nu-1}^{m_{\nu-1}},$$

where $m_1, m_2, \cdots, m_{\nu-1}$. are arbitrary rational numbers. If $m_1, m_2, \cdots, m_{\nu-1}$ were rational integers, then σ would be an integer.

It follows at once that

$$l\sigma^{(s)} = m_1 l\epsilon_1^{(s)} + m_2 l\epsilon_2^{(s)} + \cdots + m_{\nu-1} l\epsilon_{\nu-1}^{(s)} \quad (s=1, 2, \cdots, \nu-1).$$

From this system of $\nu-1$ linear homogeneous equation, since the determinant

$$L(\epsilon_1, \epsilon_2, \cdots, \epsilon_{\nu-1}) \neq 0,$$

the quantities $m_1, m_2, \cdots, m_{\nu-1}$ are uniquely determined.

Corresponding to different systems of integral exponents $m_1, m_2, \cdots, m_{\nu-1}$ the formula (1) offers different units. It is clear that there exists an infinite number of such units of the realm Ω. There may be other units in Ω. If ϵ is any such unit, put

$$l\epsilon^{(s)} = e_1 l\epsilon_1^{(s)} + e_2 l\epsilon_2^{(s)} + \cdots + e_{\nu-1} l\epsilon_{\nu-1}^{(s)} \quad (s=1, 2, \cdots, \nu-1).$$

It is seen that the real quantities $e_1, e_2, \cdots, e_{\nu-1}$ are uniquely determined. Hence, to every unit ϵ there *belongs* a definite system of real numbers $e_1, e_2, \cdots, e_{\nu-1}$.

If to the unit ϵ' there belongs the system of numbers $e_1', e_2', \cdots, e_{\nu-1}'$, then to the unit $\epsilon\epsilon'$ belongs the system $e_1+e_1', e_2+e_2', \cdots, e_{\nu-1}+e_{\nu-1}'$; and to the unit $\frac{\epsilon}{\epsilon'}$ there belongs the system $e_1-e_1', e_2-e_2', \cdots, e_{\nu-1}-e_{\nu-1}'$.

If $e_1, e_2, \cdots, e_{\nu-1}$ are all zero, then $l\epsilon', l\epsilon'', \cdots, l\epsilon^{(\nu-1)}$ are all zero; and consequently, $|\epsilon'|, |\epsilon''|, \cdots, |\epsilon^{(\nu-1)}|$ are all equal to unity.

ART. 124. Denote by S the group of units which may be brought to the form

$$\sigma = \epsilon_1^{m_1} \cdot \epsilon_2^{m_2} \cdot \cdots \cdot \epsilon_{\nu-1}^{m_{\nu-1}},$$

where $m_1, m_2, \cdots, m_{\nu-1}$ are *integral rational* numbers. It does *not* follow, if ϵ is an algebraic unit, that $m_1, m_2, \cdots, m_{\nu-1}$ are necessarily rational integers. A unit whose

corresponding exponents all lie between 0 (inclusive) and 1 (exclusive) is called a *reduced unit*, or, more definitely, *a reduced unit with regard to the group S.*

If ρ is a reduced unit with regard to the group S, then

$$\rho = \epsilon_1^{r_1}\epsilon_2^{r_2}\cdots\epsilon_{\nu-1}^{r_{\nu-1}},$$

where

$$0 \leqq r_i < 1 \qquad (i=1, 2, \cdots, \nu-1).$$

It may be proved that every unit ϵ is uniquely expressed in the form $\rho\sigma$. For, let

$$\epsilon = \epsilon_1^{e_1}\cdot\epsilon_2^{e_2}\cdot\ \cdots\ \cdot\epsilon_{\nu-1}^{e_{\nu-1}};$$

and put

$$\rho = \epsilon_1^{r_1}\epsilon_2^{r_2}\cdots\epsilon_{\nu-1}^{r_{\nu-1}},$$

$$\sigma = \epsilon_1^{m_1}\epsilon_2^{m_2}\cdots\epsilon_{\nu-1}^{m_{\nu-1}},$$

where $m_1, m_2, \cdots, m_{\nu-1}$ are rational integers, and

$$0 \leqq r_i < 1 \qquad (i=1, 2, \cdots, \nu-1).$$

It follows, if we write

$$\epsilon = \rho\sigma,$$

that

$$r_i + m_i = e_i \qquad (i=1, 2, \cdots, \nu-1);$$

and as r_i $(i=1, 2, \cdots, \nu-1)$ all lie between 0 and 1, it is clear that the integers m_i are the largest that are less than e_i $(i=1, 2, \cdots, \nu-1)$. It is seen that the m's are uniquely determined and consequently σ is uniquely determined. It also follows that

$$\rho = \frac{\epsilon}{\sigma}$$

is definitely fixed.

ART. 125. THEOREM. *The number of units belonging to Ω that are reduced with regard to the group S is finite.*

For, let ρ be a reduced unit with regard to S. Then ρ satisfies the equation of the nth degree

$$(x-\rho')(x-\rho'')\cdots(x-\rho^{(n)}) = 0;$$

or

$$x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n = 0 \qquad (a_n = \pm 1), \tag{1}$$

where $a_1, a_2, \cdots, a_n$ are rational integers, such that

$$|a_1| = |\rho' + \rho'' + \cdots + \rho^{(n)}|,$$
$$|a_2| = |\rho'\rho'' + \rho'\rho''' + \cdots + \rho^{n-1}\rho^{(n)}|, \text{ etc.}$$

Since $\rho', \rho'', \cdots, \rho^{(n)}$ lie in absolute value between certain finite limits, it is evident that

$$|\rho'|, |\rho''|, \cdots, |\rho^{(n)}|$$

are all less than g, where g is a definite finite quantity. It follows that

$$|a_1| < ng, \quad |a_2| < \binom{n}{2} g^2, \quad |a_3| < \binom{n}{3} g^3, \text{ etc.}$$

Since, further, $a_1, a_2, \cdots, a_{n-1}, a_n = \pm 1$, are rational integers, there can exist only a finite number of equations like (1), whose roots with respect to the group S are reduced units. From this it is seen that the number of reduced units with respect to the group S is finite and we may denote this number by m.

ART. **126.** Let $\rho_1, \rho_2, \cdots, \rho_m$ be the different reduced units with respect to the group S, and let ϵ be an arbitrary unit of Ω. It is evident that

$$\epsilon\rho_1, \epsilon\rho_2, \cdots, \epsilon\rho_m$$

are units, so that $\epsilon\rho_k$ may be uniquely expressed in the form $\sigma_k\tau_k$, where σ_k is a unit belonging to the group S, and τ_k is a reduced unit with respect to S $(k = 1, 2, \cdots, m)$. It follows that

$$(1) \qquad \begin{cases} \epsilon\rho_1 = \sigma_1\tau_1, \\ \epsilon\rho_2 = \sigma_2\tau_2, \\ \cdots\cdots\cdots \\ \epsilon\rho_m = \sigma_m\tau_m. \end{cases}$$

The units $\tau_1, \tau_2, \cdots, \tau_m$ are all different; for, if $\tau_1 = \tau_2$, it would follow that

$$\frac{\rho_1}{\rho_2} = \frac{\sigma_1}{\sigma_2} \qquad \text{or} \qquad \rho_1\sigma_2 = \rho_2\sigma_1.$$

But we saw (Art. 124) that every unit may be expressed as a product $\rho\sigma$ in only one way. Hence, if $\tau_1 = \tau_2$, we must also have

$$\sigma_1 = \sigma_2 \qquad \text{and} \qquad \rho_1 = \rho_2.$$

This, however, is not true, since $\rho_1, \rho_2, \cdots, \rho_m$ are all different by hypothesis. Further, as there are only m reduced units with respect to the group S, it is seen that $\tau_1, \tau_2, \cdots, \tau_m$ must, neglecting the sequence, coincide with $\rho_1, \rho_2, \cdots, \rho_m$.

If the m equations (1) are multiplied together, it is evident that

$$\epsilon^m = \sigma_1\sigma_2 \cdots \sigma_m.$$

The units $\sigma_1, \sigma_2, \cdots, \sigma_m$ all belong to the group S, the same is true of their product, which we shall call σ. It has thus been proved that

$$\epsilon^m = \sigma,$$

and with it the following important theorem: *If m is the number of units reduced with respect to the group S, the mth power of every unit that belongs to Ω is a unit belonging to the group S.*

ART. 127. Let ϵ be an arbitrary unit of the realm Ω with exponents $e_1, e_2, \cdots, e_{\nu-1}$; that is, write

$$\epsilon = \epsilon_1^{e_1}\epsilon_2^{e_2} \cdots \epsilon_{\nu-1}^{e_{\nu-1}}.$$

By virtue of the theorem of the preceding article, if m is the number of reduced units in Ω with respect to the group S, it is clear that

$$me_1 = m_1, \quad me_2 = m_2, \quad \cdots, \quad me_{\nu-1} = m_{\nu-1},$$

where $m_1, m_2, \cdots, m_{\nu-1}$ are rational integers. It follows also that $e_1, e_2, \cdots, e_{\nu-1}$ are rational numbers which have m as a common denominator.

Let the quantities $\eta_1, \eta_2, \cdots, \eta_{\nu-1}$ form another arbitrary system of independent units, so that the de-

terminant

$$\begin{vmatrix} l\eta_1', & l\eta_1'', & \cdots, & l\eta_1^{(\nu-1)} \\ l\eta_2', & l\eta_2'', & \cdots, & l\eta_2^{(\nu-1)} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ l\eta_{\nu-1}', & l\eta_{\nu-1}'', & \cdots, & l\eta_{\nu-1}^{(\nu-1)} \end{vmatrix}$$

has a positive value different from zero.

The units $\eta_1, \eta_2, \cdots, \eta_{\nu-1}$ may be expressed through the system of independent units $\epsilon_1, \epsilon_2, \cdots, \epsilon_{\nu-1}$ in the form (Art. 126)

$$\eta_s = \epsilon_1^{\frac{m_{s1}}{m}} \epsilon_2^{\frac{m_{s2}}{m}} \cdots \epsilon_{\nu-1}^{\frac{m_{s,\nu-1}}{m}} \qquad (s=1, 2, \cdots, \nu-1),$$

where $m_{s1}, m_{s2}, \cdots, m_{s,\nu-1}$ are rational integers. It follows that

$$ml\eta_s^{(t)} = m_{s1}l\epsilon_1^{(t)} + m_{s2}l\epsilon_2^{(t)} + \cdots + m_{s,\nu-1}l\epsilon_{\nu-1}^{(t)} \quad (t, s=1, 2, \cdots, \nu-1).$$

From the multiplication theorem in determinants, if we put

$$m_{st} = m_s^{(t)},$$

it is evident that

$$|ml\eta_s^{(t)}| = |m_s^{(t)}| \cdot |l\epsilon_s^{(t)}|,$$

or

$$|l\eta_s^{(t)}| = \frac{1}{m^{\nu-1}} |l\epsilon_s^{(t)}| \cdot |m_s^{(t)}| \quad (t, s=1, 2, \cdots, \nu-1).$$

Observe that $\frac{1}{m^{\nu-1}}$ and $|l\epsilon_s^{(t)}|$ are independent of the system of units $\eta_1, \eta_2, \cdots, \eta_{\nu-1}$, while upon these quantities depends the rational integer $|m_s^{(t)}|$. If, instead of $\eta_1, \eta_2, \cdots, \eta_{\nu-1}$ we choose another independent system of units, we have a different integer $|m_s^{(t)}|$. It follows that there must exist a system or systems of independent units for which this determinant has the least value. A system of independent units for which the determinant of the $(\nu-1)$st order $|m_s^{(t)}|$ takes a minimum value, is called a *fundamental system of units*, and the determinant $L(\epsilon_1, \epsilon_2, \cdots, \epsilon_{\nu-1})$ of such a system of units was called by

Dedekind the *regulator* of the system, or the regulator of the realm Ω.

ART. 128. It is now possible to prove the following important theorem: *If a unit is reduced with respect to a fundamental system of units, its exponents are all zero.*

For, let the quantities $\epsilon_1, \epsilon_2, \cdots, \epsilon_{\nu-1}$ form a fundamental system of units, so that $L(\epsilon_1, \epsilon_2, \cdots, \epsilon_{\nu-1})$ is a minimum. Let ϵ be an arbitrary unit, reduced with respect to the fundamental system, so that

$$\epsilon = \epsilon_1^{e_1}\epsilon_2^{e_2}\cdots\epsilon_{\nu-1}^{e_{\nu-1}},$$

where

$$0 \leqq e_k < 1 \qquad (k = 1, 2, \cdots, \nu-1)$$

and

$$l\epsilon^{(s)} = e_1 l\epsilon_1^{(s)} + e_2 l\epsilon_2^{(s)} + \cdots + e_{\nu-1} l\epsilon_{\nu-1}^{(s)}.$$

If it is assumed that e_1 is different from zero, it is evident that

$$\begin{aligned} e_1 L(\epsilon_1, \epsilon_2, \cdots, \epsilon_{\nu-1}) &= \begin{vmatrix} e_1 l\epsilon_1', & e_1 l\epsilon_1'', & \cdots, & e_1 l\epsilon_1^{(\nu-1)} \\ l\epsilon_2', & l\epsilon_2'', & \cdots, & l\epsilon_2^{(\nu-1)} \\ \cdots & \cdots & \cdots & \cdots \\ l\epsilon_{\nu-1}', & l\epsilon_{\nu-1}'', & \cdots, & l\epsilon_{\nu-1}^{(\nu-1)} \end{vmatrix} \\ &= \begin{vmatrix} \sum_{i=1}^{\nu-1} e_i l\epsilon_i', & \sum_{i=1}^{\nu-1} e_i l\epsilon_i'', & \cdots, & \sum_{i=1}^{\nu-1} e_i l\epsilon_i^{(\nu-1)} \\ l\epsilon_2', & l\epsilon_2'', & \cdots, & l\epsilon_2^{(\nu-1)} \\ \cdots & \cdots & \cdots & \cdots \\ l\epsilon_{\nu-1}', & l\epsilon_{\nu-1}'', & \cdots, & l\epsilon_{\nu-1}^{(\nu-1)} \end{vmatrix} \\ &= \begin{vmatrix} l\epsilon', & l\epsilon'', & \cdots, & l\epsilon^{(\nu-1)} \\ l\epsilon_2', & l\epsilon_2'', & \cdots, & l\epsilon_2^{(\nu-1)} \\ \cdots & \cdots & \cdots & \cdots \\ l\epsilon_{\nu-1}', & l\epsilon_{\nu-1}'', & \cdots, & l\epsilon_{\nu-1}^{(\nu-1)} \end{vmatrix} \\ &= L(\epsilon', \epsilon_2', \cdots, \epsilon_{\nu-1}'). \end{aligned}$$

Since

$$0 \leqq e_1 < 1,$$

it follows that

$$L(\epsilon_1, \epsilon_2, \cdots, \epsilon_{\nu-1}) > L(\epsilon', \epsilon_2', \cdots, \epsilon_{\nu-1}'),$$

which contradicts the definition of a fundamental system. It follows that

$$e_1 = 0;$$

and similarly, it may be shown that

$$e_2 = 0 = e_3 = \cdots = e_{\nu-1}.$$

ART. **129.** In the expression

$$\sigma = \epsilon_1^{m_1}\epsilon_2^{m_2}\cdots\epsilon_{\nu-1}^{m_{\nu-1}}$$

observe that two different sets of values of $m_1, m_2, \cdots, m_{\nu-1}$ always offer two different σ's. Otherwise, there would be a linear relation among the quantities $l\epsilon_1, l\epsilon_2, \cdots, l\epsilon_{\nu-1}$, whose determinant is zero, and this contradicts the definition of a system of independent units.

Let ρ be a unit reduced with respect to the fundamental system of units $\epsilon_1, \epsilon_2, \cdots, \epsilon_{\nu-1}$ and suppose that m is the number of these reduced units with respect to $\epsilon_1, \epsilon_2, \cdots, \epsilon_{\nu-1}$; then (Art. 127)

$$\rho^m = \epsilon_1^{m_1}\cdot\epsilon_2^{m_2}\cdot\ \cdots\ \cdot\epsilon_{\nu-1}^{m_{\nu-1}},$$

where $m_1, m_2, \cdots, m_{\nu-1}$ are rational integers; and that is, ρ^m is a unit that belongs to the group S. But, from the theorem of the preceding article, the integers $m_1, m_2, \cdots, m_{\nu-1}$ are all zero. It follows then that

$$\rho^m = 1,$$

and with this we may state the following theorem: *Every unit that is reduced with respect to a fundamental system of units is an mth root of unity.*

If ϵ_0 is a primitive mth root of unity, all the m mth roots of unity are had from $\epsilon_0^{m_0}$, where m_0 goes through a complete system of residues (mod. m).

ART. **130.** Let $\epsilon_1, \epsilon_2, \cdots, \epsilon_{\nu-1}$ be a system of independent units. In Art. 124 it was seen that every arbitrary unit of the realm Ω may be expressed in the form $\rho\sigma$, where σ is a unit belonging to the group S; and

where ρ is a unit reduced with respect to S. It was seen that this representation is unique.

Since ρ may be expressed in the form $\epsilon_0^{m_0}$, where m_0 is an integer uniquely determined (mod. m) and ϵ_0 is a primitive mth root of unity and, since σ has the form

$$\sigma = \epsilon_1^{m_1}\epsilon_2^{m_2} \cdot \cdots \cdot \epsilon_{\nu-1}^{m_{\nu-1}},$$

where $m_1, m_2, \cdots, m_{\nu-1}$ are arbitrary rational integers, the theorem of Art. 111 is proved.

ART. 131. Observe that in the Dirichlet-Dedekind treatment of algebraic units, there are emphasized three fundamental theorems, due to which it is proved (1) that there exists a unit through which it is possible to determine other units that are independent of one another; (2) that there are a finite number of independent units which, raised to rational powers, generate all other units of the realm; and (3) that among the different systems of such independent units there exists a fundamental system, integral powers of which produce *all* the units of the realm.

Bachmann indicates that the theory, as sketched by Dirichlet, was developed in full by him.[1] His derivations of the results of Arts. 122 ff. are of much interest and will be reproduced here.

Note if $\mathfrak{a}$ is any ideal, that $\frac{\mathfrak{a}}{\mathfrak{a}} = \mathfrak{a}^0$ is an order-modul. And since $[1] = \mathfrak{z} > \mathfrak{a}^0$, it follows (Vol. I, Art. 132) that $\mathfrak{a}^0\mathfrak{o} = \mathfrak{o}$, that $\mathfrak{a}\mathfrak{a}^0 = \mathfrak{a} = \frac{\mathfrak{a}}{\mathfrak{a}^0}$ and $\mathfrak{a}^0\mathfrak{a}^0 = \mathfrak{a}^0 = \frac{\mathfrak{a}^0}{\mathfrak{a}^0}$.

We shall at first limit the discussion to any order-modul $\mathfrak{o}_1$. It will become evident that similar results exist for $\mathfrak{o}$ as have been found for $\mathfrak{o}_1$. Let $\tilde{\omega}_1, \tilde{\omega}_2, \cdots, \tilde{\omega}_n$

[1] P. Bachmann, *Allgemeine Arithmetik*, footnote, p. 322; also, "De unitatum complexarum theoria," *Inaug. Diss.*, Berlin, 1864.

be any basis of $\mathfrak{o}_1$ so that

$$\mathfrak{o}_1 = [\tilde{\omega}_1, \tilde{\omega}_2, \cdots, \tilde{\omega}_n].$$

It is seen by giving to the indeterminates u all rational integral values in the expression

$$\tilde{\omega} = u_1\tilde{\omega}_1 + u_2\tilde{\omega}_2 + \cdots + u_n\tilde{\omega}_n, \tag{1}$$

that all the integers of $\mathfrak{o}_1$ are had. It follows, if ω is an integer of the order-modul, that $\tilde{\omega}\tilde{\omega}_1, \tilde{\omega}\tilde{\omega}_2, \cdots, \tilde{\omega}\tilde{\omega}_n$ are also integers of $\mathfrak{o}_1$. We may accordingly write

$$\tilde{\omega}\tilde{\omega}_i = a_{i1}\tilde{\omega}_1 + a_{i2}\tilde{\omega}_2 + \cdots + a_{in}\tilde{\omega}_n \quad (i=1, 2, \cdots, n), \tag{2}$$

where the determinant of the rational integers a is (Vol. I, Art. 59) the norm of $\tilde{\omega}$.

It follows from solving the equations (2) that the product $N(\tilde{\omega})\tilde{\omega}_i$ and therefore also the product of $N(\tilde{\omega})$ by any integer of $\mathfrak{o}_1$, say $N(\tilde{\omega})\tilde{\omega}'$ is an integer of the form

$$\tilde{\omega}(A_1\tilde{\omega}_1 + A_2\tilde{\omega}_2 + \cdots + A_n\tilde{\omega}_n).$$

With this it is seen that the product $\dfrac{N(\tilde{\omega})}{\tilde{\omega}}\tilde{\omega}'$, where $\tilde{\omega}'$ is any integer of $\mathfrak{o}_1$, is an integer of $\mathfrak{o}_1$.

And it follows, *since ± 1 is an integer of $\mathfrak{o}_1$, that, if ϵ is a unit in $\mathfrak{o}_1$ whose norm is ± 1, then also $\dfrac{1}{\epsilon}$ is an integer of $\mathfrak{o}_1$.*

ART. 132. We may next prove the *existence of units* in $\mathfrak{o}_1$. Let the fixed realm $\Omega = \Re(\theta)$ be generated by θ, where θ is a root of the irreducible equation $F(x) = 0$. Let $\theta = \theta^{(1)}, \theta^{(2)}, \cdots, \theta^{(n)}$ be the conjugate roots of this equation. Of these roots, as in Art. 112, let there be r real, namely $\theta^{(1)}, \theta^{(2)}, \cdots, \theta^{(r)}$ and q pairs of conjugate roots $\theta^{(r+1)}, \theta^{(r+q+1)}; \theta^{(r+2)}, \theta^{(r+q+2)}; \cdots; \theta^{(r+q)}, \theta^{(r+2q)}$, so that $n = r + 2q$.

When for $\theta = \theta^{(1)}$ are written its conjugate values, the form $\tilde{\omega}$ above, becomes

$$\tilde{\omega}^{(i)} = u_1\tilde{\omega}_1^{(i)} + u_2\tilde{\omega}_2^{(i)} + \cdots + u_n\tilde{\omega}_n^{(i)} \quad (i=1, 2, \cdots, n).$$

Write

$$f_i = \tilde{\omega}^{(i)} \qquad (i=1, 2, \cdots, r);$$

$$(1) \qquad \begin{cases} f_{r+k} = \dfrac{\tilde{\omega}^{(r+k)} + \tilde{\omega}^{(r+q+k)}}{\sqrt{2}}, \\ f_{r+q+k} = \dfrac{\tilde{\omega}^{(r+k)} - \tilde{\omega}^{(r+q+k)}}{i\sqrt{2}} \qquad (k=1, 2, \cdots, q), \end{cases}$$

which become the n linear forms with real coefficients

$$f_1 = u_1\tilde{\omega}^{(1)} + u_2\tilde{\omega}_2^{(1)} + \cdots + u_n\tilde{\omega}_n^{(1)},$$
$$f_2 = u_1\tilde{\omega}^{(2)} + u_2\tilde{\omega}_2^{(2)} + \cdots + u_n\tilde{\omega}_n^{(2)},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$f_r = u_1\tilde{\omega}^{(r)} + u_2\tilde{\omega}_2^{(r)} + \cdots + u_n\tilde{\omega}_n^{(r)};$$
$$f_{r+1} = u_1\frac{\tilde{\omega}_1^{(r+1)} + \tilde{\omega}_1^{(r+q+1)}}{\sqrt{2}} + \cdots + u_n\frac{\tilde{\omega}_n^{(r+1)} + \tilde{\omega}_n^{(r+q+1)}}{\sqrt{2}},$$
$$f_{r+2} = u_1\frac{\tilde{\omega}_1^{(r+2)} + \tilde{\omega}_1^{(r+q+2)}}{\sqrt{2}} + \cdots + u_n\frac{\tilde{\omega}_n^{(r+2)} + \tilde{\omega}_n^{(r+q+2)}}{\sqrt{2}},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$f_{r+q+1} = u_1\frac{\tilde{\omega}_1^{(r+1)} - \tilde{\omega}_1^{(r+q+1)}}{i\sqrt{2}} + \cdots + u_n\frac{\tilde{\omega}_n^{(r+1)} - \tilde{\omega}_n^{(r+q+1)}}{i\sqrt{2}},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots.$$

Observe that the determinant of these forms is the square root of the discriminant D_1, where D_1 is the fundamental invariant of the order-modul $\mathfrak{o}_1$.

To the indeterminates u_i in the above expressions give rational integral values a_i. The forms f_i become conjugate algebraic integers belonging respectively to the n conjugate realms. Next give to each of these integers a_i values not greater than a fixed positive integer k, where k is to be determined later. Further, denote the absolute values of the coefficients of the u's in the expressions for f_i by $v_h^{(i)}$, so that

$$|f_i| \leqq k(v_1^{(i)} + v_2^{(i)} + \cdots + v_n^{(i)}) \qquad (i=1, 2, \cdots, n).$$

Finally, let G be the greatest of these n sums. It is

evident that

$$|f_i| \gtrless kG \qquad (i=1, 2, \cdots, n). \tag{2}$$

Observe that G does *not* depend upon k but upon the basal elements of $\mathfrak{o}_1$.

Next distribute the n functional values $|f_i|$ into two groups A and B in such a way that there is at least one f in either group and always the two functional values f_{r+i}, f_{r+q+i} must fall within the same group.

Let s denote the number of the f's that fall in the first group so that $n-s$ is the number that occur in the second group. Since $k>0$ and $n>s>0$, it is clear that

$$(k+1)^{\frac{n}{s}} - k^{\frac{n}{s}} > 1;$$

and consequently there exists a positive integer m, such that

$$(k+1)^{\frac{n}{s}} > m > k^{\frac{n}{s}},$$

or

$$(k+1)^n > m^s > k^n.$$

Define d by the relation

$$d = \frac{2Gk}{m}$$

and observe that

$$d < 2Gk^{1-\frac{n}{s}}. \tag{3}$$

Next divide the interval $-kG \cdots +kG$ into the following m partial intervals each of the length d,

$$\begin{aligned} &-kG,\ -kG+d;\ -kG+d,\ -kG+2d;\ \cdots, \\ &\qquad -kG+(m-1)d,\ -kG+md(=kG). \end{aligned} \tag{4}$$

Observe that the rational integral values that are chosen for the u's in formula (1) may have any of the values 0, 1, $\cdots$, k, so that there are $(k+1)^n$ different choices. The s functions f which belong to group A fall in the m intervals (4). Since each of them may fall in each of the m

intervals, there are m^s possible distributions of the f's, that belong to group A. And this number m^s is less than $(k+1)^n$, which is the number of ways that the u's may be chosen. It follows, when the u's are chosen in all possible ways, that the distribution of the f's of the group A must be such that they occur at least twice in the same intervals (4). Suppose that this happens for the two systems of values $u_i=a_i'$ and $u_i=a_i''$ $(i=1, 2, \cdots, n)$, and denote the corresponding f's by f' and f''. Next give to u_i the values

$$u_i=a_i'-a_i'', \tag{5}$$

and observe that the n functions

$$f_i=f_i'-f_i'' \qquad (i=1, 2, \cdots, n)$$

which belong to the group A, since they fall within the same interval, are in numerical value less than d.

Due to formulas (1), we have

$$\tilde{\omega}^{(i)}=f_i \qquad (i=1, 2, \cdots, r)$$

and

$$\tilde{\omega}^{(r+k)}=\frac{f_{r+k}+if_{r+q+k}}{2}, \qquad \tilde{\omega}^{(r+q+k)}=\frac{f_{r+q}-if_{r+q+k}}{2}$$
$$(k=1, 2, \cdots, q).$$

Observe that the absolute values of $\tilde{\omega}^{(r+k)}$ and $\tilde{\omega}^{(r+q+k)}$ are the square roots of $\frac{f_{r+k}^2+f_{r+q+k}^2}{2}$. With the limitations thus made, it is seen that those of the functional values $\tilde{\omega}^{(i)}$ which belong to the group A satisfy the inequality

$$|\tilde{\omega}^{(i)}|<d, \tag{6}$$

while due to (2), those which belong to group B satisfy the inequality

$$|\tilde{\omega}^{(i)}|\leqq kG. \tag{7}$$

It follows that if we give the values (5) to the u's, the $\tilde{\omega}$ of formula (1) of the preceding article becomes an algebraic integer of $\mathfrak{o}_1$, and due to the inequalities (6) and

(7), it is seen that the product P of those $\tilde{\omega}^{(i)}$ which belong to group A is less than d^s, while the product Q of those $\tilde{\omega}^{(i)}$ which belong to group B is not greater than $(kG)^{n-s}$, so that finally

$$|PQ| = |N(\tilde{\omega})| < d^{\sigma}(kG)^{n-\sigma},$$

or, from (3)

$$|N(\tilde{\omega})| < (2G)^n.$$

Since the norm of every algebraic integer is in absolute value $\overline{\geqq} 1$, it follows that

$$|PQ| \overline{\geqq} 1$$

and therefore

$$|Q| \overline{\geqq} \frac{1}{P} > d^{-s}.$$

If $\tilde{\omega}^{(i)}$ is any one of the conjugates of group B and as the product of the remaining $n-s-1$ of this group, due to (7), is not greater than $(kG)^{n-s-1}$, it is seen that

$$|\tilde{\omega}^{(i)}| \overline{\geqq} \frac{Q}{(kG)^{n-s-1}}.$$

Further, since $Q > d^{-s}$, and that is, from (3)

$$Q > \frac{k^{n-s}}{(2G)^s}$$

it follows, since $n > s$, that

$$|\tilde{\omega}^{(i)}| > \frac{k}{2^s G^{n-1}} > \frac{k}{(2G)^{n-1}}. \tag{8}$$

Due to formula (3) the positive integer k may be taken so large that d may be made smaller than any arbitrary quantity however small, while at the same time $\frac{k}{(2G)^{n-1}}$ may be made greater than any arbitrary quantity however large.

Observing (6) and (8), it is seen that the above results may be formulated in the theorem: *In any order* $\mathfrak{o}_1$ *there exists an integer* $\tilde{\omega}$ *for which those conjugate values* $\tilde{\omega}^{(i)}$

which belong to group A are in absolute value less than a fixed quantity a however small, while those of the $\tilde{\omega}^{(i)}$ *which belong to group B are in absolute value greater than an arbitrary value b, however large, and at the same time* $|N(\tilde{\omega})| < (2G)^n$.

ART. **133.** It follows from the above theorem that there exists an integer α in $\mathfrak{o}_1$ whose norm in absolute value is less than $(2G)^n$, and further there exists in $\mathfrak{o}_1$ an integer β whose norm in absolute value is less than $(2G)^n$ and whose conjugates $\beta^{(i)}$ which belong to group A are all less than the absolute value of the smallest $\alpha^{(i)}$ in group A, while all those conjugates $\beta^{(i)}$ which belong to group B are all greater than the greatest $\alpha^{(i)}$ of group B. Continuing this process, we can form an indefinitely large number of integers

$$\alpha, \beta, \gamma, \cdots, \lambda, \cdots, \mu, \cdots \tag{1}$$

whose norms in absolute value are less than $(2G)^n$, while all those conjugates of μ that belong to group A are less than the smallest of the conjugates of λ which belong to A; and all those conjugates $\mu^{(i)}$ which belong to group B are greater than the largest of the conjugates $\lambda^{(i)}$ which belong to group B. Since, however, the norms of algebraic integers are rational integers, and there being only a finite number of rational integers that are less than $(2G)^n$, it follows that an indefinitely large number of the integers (1) must have the same norm, say N. Further, since all the integers (1) are of the form

$$\tilde{\omega} = u_1\tilde{\omega}_1 + u_2\tilde{\omega}_2 + \cdots + u_n\tilde{\omega}_n,$$

when rational integral values are given to the u's, it is clear, when these integers are considered, modulo N, that there are only N^n different integers $\tilde{\omega}$, and accordingly, that of the integers (1) there must be at least two, say λ and μ which are congruent, modulo N. And that

is,

$$\lambda - \mu = N\tilde{\omega}^1,$$

where λ, μ and $\tilde{\omega}^1$ are all integers of $\mathfrak{o}_1$.

It follows that

$$\frac{\lambda}{\mu} = 1 + \frac{N}{\mu}\tilde{\omega}^1 = 1 + \frac{N(\mu)}{\mu}\tilde{\omega}^1.$$

Further, see Art. 131, the right hand side of this expression is an integer in $\mathfrak{o}_1$. If then we put $\frac{\lambda}{\mu} = \epsilon$, it is seen that ϵ is an integer in $\mathfrak{o}_1$ whose norm is $+1$, since $N(\lambda) = N(\mu) = N$, and at the same time (*loc. cit.*) $\frac{1}{\epsilon}$ is an integer of $\mathfrak{o}_1$.

Observing that μ comes after λ in the sequence (1) it follows from the method by which these integers were formed that *all the conjugates* $\epsilon^{(i)}$ *which belong to group A are in absolute value* >1, *while those conjugates* $\epsilon^{(i)}$ *which belong to group B are in absolute value* <1.

The same results are at once established for the order modul $\mathfrak{o}$ of any fixed realm if instead of the basal elements $\tilde{\omega}_1, \tilde{\omega}_2, \cdots, \tilde{\omega}_n$ of $\mathfrak{o}_1$, we write the basal elements $\omega_1, \omega_2, \cdots, \omega_n$ of $\mathfrak{o}$. With this is proved the theorem as stated by Bachmann (*op. cit.*, p. 331): *In every order modul* $\mathfrak{o}_1$ *including* $\mathfrak{o}$ *of a fixed realm, there exists a unit* ϵ *with positive norm such that in absolute values those conjugates* $\epsilon^{(i)}$ *which belong to group A are greater than 1 while those conjugates of group B are all less than 1.*

ART. **134.** Another derivation of this theorem is given by Minkowski (*Göttingen Nachrichten*, 1900, p. 90; *Collected Works*, Vol. I, p. 316). It depends upon the following theorem in determinants:

If in the determinant

$$|a_{ik}| \qquad (i, k = 1, 2, \cdots, m)$$

with real elements, all the terms save those of the principal diagonal are negative, while the sum of the terms in every row is positive, the value of the determinant is positive.

For $m=1$, the determinant is the positive quantity a_{11}. If $m=2$, with the assumption that

$$s_1=a_{11}+a_{12}, \qquad s_2=a_{21}+a_{22}$$

are positive, it is seen that

$$|a_{ik}|=a_{22}s_1-a_{12}s_2,$$

which is positive.

Suppose then that the theorem is true for determinants of degree less than m, and write in the determinant $|a_{ik}|$ for a_{hh} the sum $s_h+\sigma_{hh}$, where σ_{hh} is a positive quantity, since $a_{hh}>s_h$. Observe that

$$(1) \qquad a_{h1}+a_{h2}+\cdots+\sigma_{hh}+\cdots+a_{hm}=0 \quad (h=1, 2, \cdots, m),$$

and accordingly that the determinant

$$\begin{vmatrix} \sigma_{11}, & a_{12}, & \cdots, & a_{1m} \\ a_{21}, & \sigma_{22}, & \cdots, & a_{2m} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ a_{m1}, & a_{m2}, & \cdots, & a_{mm} \end{vmatrix} =0,$$

since the sum of the elements of any row may be written for the first element and this sum is zero.

Develop the determinant

$$|a_{ik}|=\begin{vmatrix} s_1+\sigma_{11}, & a_{12}, & \cdots, & a_{1m} \\ a_{21}, & s_2+\sigma_{22}, & \cdots, & a_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1}, & a_{m2}, & \cdots, & s_m+\sigma_{mm} \end{vmatrix}$$

with respect to the quantities s_i. It follows from above that the determinant independent of the s's is zero, the coefficient of $s_1s_2\cdots s_m$ is unity, and by hypothesis s_1, s_2, $\cdots$, s_m are all positive; the coefficient of any other term

say $s_1 s_2$ is the determinant

$$\begin{vmatrix} \sigma_{33}, & a_{34}, & \cdots, & a_{3m} \\ a_{43}, & \sigma_{44}, & \cdots, & a_{4m} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m3}, & a_{m4}, & \cdots, & \sigma_{mm} \end{vmatrix},$$

where the elements outside of the principal diagonal are all negative, while the sum of the rows, due to (1), are all positive and the determinant, being of less degree than m, is by hypothesis positive. Accordingly all the terms in this development are positive, which renders the given determinant positive.

To make an application of this theorem, observe next that if $\epsilon^{(1)}, \epsilon^{(2)}, \cdots, \epsilon^{(\nu)}$ are any conjugate values of the unit ϵ, and if their logarithms in absolute value (Art. 121) are denoted by

$$l_1(\epsilon), l_2(\epsilon), \cdots, l_\nu(\epsilon),$$

then at pleasure (Art. 122) one of these logarithms may be taken positive and all the others negative. Accordingly, we may determine $m = \nu - 1$ units $\epsilon_1, \epsilon_2, \cdots, \epsilon_m$ such that $l_1(\epsilon_1), l_2(\epsilon_2), \cdots, l_m(\epsilon_m)$ are positive, while all the other logarithms are negative. Due to the formula

$$l_1(\epsilon_i) + l_2(\epsilon_i) + \cdots + l_\nu(\epsilon_i) = 0,$$

it follows that

$$l_1(\epsilon_i) + l_2(\epsilon_i) + \cdots + l_m(\epsilon_i) > 0, \quad (i = 1, 2, \cdots, m).$$

Accordingly, it follows from the theorem of this article that

$$\begin{vmatrix} l_1(\epsilon_1), & l_2(\epsilon_1), & \cdots, & l_m(\epsilon_1) \\ l_1(\epsilon_2), & l_2(\epsilon_2), & \cdots, & l_m(\epsilon_2) \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ l_1(\epsilon_m), & l_2(\epsilon_m), & \cdots, & l_m(\epsilon_m) \end{vmatrix}$$

is positive.

From this it is seen that the units $\epsilon_1, \epsilon_2, \cdots, \epsilon_m$ form a system of $m = \nu - 1$ independent units of the order-modul $\mathfrak{o}$.

Observe that, whereas in Art. 122 the method given by Dirichlet for the determination of such a system of independent units requires the formation of certain determinants which are composed of successively derived units, here the derivation of the single units as given in Art. 133 is done directly and in an independent manner.

II. The Hilbert-Minkowski Exposition

Art. **135.** The following fundamental Lemmas due to Minkowski were proved Vol. I, in Arts. 26 ff. The proof for n variables due to Minkowski is found in Art. 147. See also Hilbert, *Bericht*, Chap. VI.

Lemma I. *If*

$$f_1 = a_{11}u_1 + \cdots + a_{1n}u_n,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$f_n = a_{n1}u_1 + \cdots + a_{nn}u_n,$$

are n linear homogeneous forms in $u_1, \cdots, u_n$ with arbitrary real coefficients $a_{11}, \cdots, a_{nn}$, whose determinant $=1$, it is always possible to give to $u_1, \cdots, u_n$ rational integral values that are not all zero, and such that the absolute values of the n forms just written are all $\leqq 1$.

Lemma II. *If $f_1, \cdots, f_n$ are n linear homogeneous forms in $u_1, \cdots, u_n$ with arbitrary real coefficients and with positive determinant A, and if $k_1, \cdots, k_n$ are arbitrary positive quantities, whose product $= A$, it is possible always to give to $u_1, \cdots, u_n$ integral rational values which are not all zero and such that the absolute values of the n forms above satisfy the conditions*

$$|f_1| \leqq k_1, \cdots, |f_n| \leqq k_n.$$

Deviating from our previous notation, write $\Omega = \Omega'$, so that the n conjugate realms are $\Omega', \Omega'', \cdots, \Omega^{(n)}$. Lemma II may be used to prove the following theorem.

Theorem. *Let $k_1, \cdots, k_n$ be n real positive constants whose product is equal $|\sqrt{D}|$, and which satisfy the*

conditions $k_s = k_{s'}$, *if* $\Omega^{(s)}$ *and* $\Omega^{(s')}$ *are conjugate complex realms. It is always possible to determine in the realm* Ω *an integer* ω, *which is not zero and such that its conjugates*

$$|\omega^{(1)}| \leqq k_1, \cdots, |\omega^{(n)}| \leqq k_n.$$

Proof. Corresponding to the realms $\Omega^{(1)}, \cdots, \Omega^{(n)}$, let there be arranged linear forms which satisfy the following requirements:

If $\Omega^{(r)}$ is a real realm, write

$$f_r = \omega_1^{(r)} u_1 + \cdots + \omega_n^{(r)} u_n;$$

if however, $\Omega^{(s)}$ and $\Omega^{(s')}$ are conjugate complex realms, write

$$f_s = \frac{1}{\sqrt{2}}\{(\omega_1^{(s)} + \omega_1^{(s')})u_1 + \cdots + (\omega_n^{(s)} + \omega_n^{(s')})u_n\},$$

$$f_{s'} = \frac{1}{i\sqrt{2}}\{(\omega_1^{(s)} - \omega_1^{(s')})u_1 + \cdots + (\omega_n^{(s)} - \omega_n^{(s')})u_n\},$$

and observe that all the coefficients are real.

Note that the absolute value of the determinant of the n forms as above constructed is $= |\sqrt{D}|$. The proof follows from Lemma II, if we observe that on the one hand

$$|f_s' + if_{s'}'|^2 = (\sqrt{f_s^2 + f_{s'}^2})^2 \leqq k_s^2 + k_s^2 = 2k_s^2,$$

and on the other hand,

$$|f_s + if_{s'}|^2 = 2|\omega_1^{(s)} u_1 + \cdots + \omega_n^{(s)} u_n|^2,$$
$$|f_s - if_{s'}|^2 = 2|\omega_1^{(s')} u_1 + \cdots + \omega_n^{(s')} u_n|^2.$$

The following theorem was proved in Art. 125, end.

THEOREM. *If* k *is an arbitrary positive constant, there are only a finite number of algebraic integers which together with their conjugates are in absolute value* $< k$.

ART. **136.** Theorems regarding the absolute value of the discriminant of the realm are:

THEOREM I. *The discriminant* D *of the realm* Ω *is always different*[1] *from* ± 1. The proof is given below.

[1] Minkowski's proofs of these theorems are found in Art. 149.

THEOREM II. *There are only a finite number of realms of the nth degree that have a given discriminant D.*

This theorem was proved by Hermite: "Sur la theorie des formes etc.," *Crelle*, Vol. 47, p. 335.

In the proof of the above theorem we must use the following lemma:

LEMMA. *If* $f_1, \cdots, f_n$ *are the linear forms in* $u_1, \cdots, u_n$ *that were given in the proof of the theorem of the preceding article, there always exists in* Ω *an integer* $(\neq 0)$, *say* $\alpha = a_1\omega_1 + \cdots + a_n\omega_n$, *whose conjugate values for* $u_1 = a_1, \cdots, u_n = a_n$, *satisfy the conditions*

$$|f_1| \leqq |\sqrt{D}|, \ |f_2| < 1, \ \cdots, \ |f_n| < 1. \tag{1}$$

Observe that in the theorem of the preceding article the equality sign also occurs with the expressions just written.

From the theorem of Art 147 it will be seen that there are only a finite number of algebraic integers in Ω say α, $\alpha_1, \alpha_2, \cdots$, which satisfy the conditions

$|f_1| < |\sqrt{D}| + k$, where k is a positive quantity,
$|f_2| < 1, \ \cdots, \ |f_n| < 1.$

Let α be the integer for which $|f_1|$ has the smallest value and let φ denote *this* smallest value. If $k = 0$, then φ satisfies the postulates of the Lemma.

If φ is not $\leqq |\sqrt{D}|$, determine a positive number ϵ such that $(1+\epsilon)^{n-1}|\sqrt{D}| < \varphi$. Due to Theorem I of the preceding article, it is always possible to determine a system of positive rational integers for $u_1, \cdots, u_n$ such that

$$|f_1| \leqq (1+\epsilon)^{n-1}|\sqrt{D}|, \ f_2 \leqq \frac{1}{1+\epsilon}, \ \cdots, \ f_n \leqq \frac{1}{1+\epsilon},$$

and consequently

$$|f_1| < \varphi, \ |f_2| < 1, \ \cdots, \ |f_n| < 1.$$

But f_1 cannot be less than φ, as by hypothesis φ was the smallest value that f_1 may take.

To prove Theorem I we proceed as follows: If $\Omega^{(1)}$ is a real realm, the form f_1 is definitely determined; if, however, $\Omega^{(1)}$ is a complex imaginary realm and if $\Omega^{(2)}$ is conjugate to it, there is a choice of two forms for f_1. In this case put

$$f_1 = \frac{1}{i\sqrt{2}}\{(\omega_1^{(1)} - \omega_1^{(2)})u_1 + \cdots + (\omega_n^{(1)} - \omega_n^{(2)})u_n\}.$$

The other forms $f_2, \cdots, f_n$, may be taken in any sequence. Due to formulas (1) there exists an integer α, such that $|\alpha'| \leqq |\sqrt{D}|$, while $|\alpha''| < 1, \cdots, |\alpha^n| < 1$.

Observe next that

$$|N(\alpha)| = \prod_r |f_r| \prod_{s,s'} \frac{f_s^2 + f_{s'}^2}{2},$$

where the first product is taken over all real forms f_r, while the second product is over all pairs of conjugate complex imaginary forms $f_s, f_{s'}$.

Since $|N(\alpha)| \geqq 1$, it follows that $|f_1| > 1$, and consequently also $|\sqrt{D}| > 1$. And accordingly Theorem I is proved.

From the conditions $|f_1| > 1$, $|f_2| < 1, \cdots, |f_n| < 1$, it is evident that α is an integer of Ω which is different from all its conjugates and therefore (Vol. I, Art. 61) α determines the realm Ω. As $|\sqrt{D}|$ is fixed it follows from the relations (1) that there are only a finite number of algebraic integers α which satisfy the conditions just written. And this offers an immediate proof of Theorem II.

From these theorems it is seen that the discriminant of every realm must contain at least one prime integer as a factor. It follows immediately that there are only a finite number of realms of finite degree which have a fixed discriminant D.

More definite limits for the discriminant of a fixed realm are found in Art. 149.

ART. **137.** THEOREM. *If* $\mathfrak{a}$ *is a given ideal of the realm* Ω, *there is always an integer* α *that is divisible by* $\mathfrak{a}$ *and whose norm satisfies the condition*

$$|N(\alpha)| \leqq N(\mathfrak{a})|\sqrt{D}|.$$

(See Minkowski, *Werke*, Vol. I, p. 258.)

Proof. Let

$$\begin{aligned} \alpha_1 &= a_{11}\omega_1 + \cdots + a_{1n}\omega_n, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ \alpha_n &= a_{n1}\omega_1 + \cdots + a_{nn}\omega_n, \end{aligned}$$

constitute the basis of the ideal $\mathfrak{a}$.

As in Art. 136 write

$$f_r = \alpha_1^{(r)}u_1 + \cdots + \alpha_n^{(r)}u_n,$$

for real realms, and

$$f_s = \frac{1}{\sqrt{2}}\{(\alpha_1^{(s)} + \alpha_1^{(s')})u_1 + \cdots + (\alpha_n^{(s)} + \alpha_n^{(s')})u_n\}$$

$$f_{s'} = \frac{1}{i\sqrt{2}}\{(\alpha_1^{(s)} - \alpha_1^{(s')})u_1 + \cdots + (\alpha_n^{(s)} - \alpha_n^{(s')})u_n\}$$

for pairs of conjugate complex realms.

Observe that the determinant of the n real forms thus constructed is

$$A = \begin{vmatrix} \alpha_1^{(1)}, & \cdots, & \alpha_n^{(1)} \\ \cdots\cdots & & \cdots\cdots \\ \alpha_1^{(n)}, & \cdots, & \alpha_n^{(n)} \end{vmatrix} = \begin{vmatrix} a_{11}, & \cdots, & a_{1n} \\ \cdots\cdots & & \cdots\cdots \\ a_{n1}, & \cdots, & a_{nn} \end{vmatrix} \begin{vmatrix} \omega_1^{(1)}, & \cdots, & \omega_n^{(1)} \\ \cdots\cdots & & \cdots\cdots \\ \omega_1^{(n)}, & \cdots, & \omega_n^{(n)} \end{vmatrix},$$

which in absolute value (Art. 11) is $= |N(\mathfrak{a})\sqrt{D}|$. Next take any n positive constants $k_1, \cdots, k_n$, whose product is equal to the determinant A, the only restriction being that $k_s = k_{s'}$, when $\Omega^{(s)}$ and $\Omega^{(s')}$ are a pair of conjugate complex realms. Determine by the Minkowski Theorem rational integers $a_1, \cdots, a_n$, which when substituted in the n forms $f_1, \cdots, f_n$ cause these forms to be respectively

$\leqq$ the constants $k_1, \cdots, k_n$. The number α, which with its conjugate values is represented through the forms $f_1, \cdots, f_n$, has the property required in the theorem.

ART. **138.** The following articles are in great measure the work of Minkowski (*Geometrie der Zahlen*, §§ 44 et seq.; see also Hilbert, *Bericht*, §§ 19–21). They present the Dirichlet Theory of Units in a way somewhat different from that given above. The Hilbert statement and proof of the Dirichlet Theorem is as follows:

THEOREM. *If among the n conjugate realms* $\Omega^{(1)}, \cdots, \Omega^{(n)}$, *there are* r_1 *real realms and* $r_2 = \frac{n-r_1}{2}$ *pairs of complex imaginary realms, there is a system of* $r = r_1 + r_2 - 1$ *units* $\epsilon_1, \cdots, \epsilon_r$ *in the realm* $\Omega = \Omega^{(1)}$ *such that every other unit* ϵ *of this realm may be expressed in one and only one way in the form*

$$\epsilon = \rho \epsilon_1^{a_1} \cdots \epsilon_r^{a_r},$$

where $a_1, \cdots, a_r$ *are rational integers and where* ρ *is a definite root of unity which appears in* Ω.

As a preparation for the proof of this theorem, arrange the n conjugate realms $\Omega^{(1)}, \cdots, \Omega^{(n)}$ as follows: Write down the r_1 real realms $\Omega^{(1)}, \cdots, \Omega^{(r_1)}$; then choose one realm from each of the pairs of conjugate complex realms; denote these by $\Omega^{(r_1+1)}, \cdots, \Omega^{(r_1+r_2)}$; and then let follow the realms $\Omega^{(r_1+r_2+1)}, \cdots, \Omega^{(n)}$, which are the conjugates of the complex realms. Next form with the n indeterminates $u_1, \cdots, u_n$, the n linear forms

$$\xi_s = \omega_1^{(s)} u_1 + \cdots + \omega_n^{(s)} u_n \qquad (s = 1, 2, \cdots, n),$$

where $\xi_1 = \xi$, and where $\omega_1^{(s)}, \omega_2^{(s)}, \cdots, \omega_n^{(s)}$ constitute a basis of $\Omega^{(s)}$. The quantities $\xi_1, \cdots, \xi_n$ being different from zero, write, when $\Omega^{(s)}$ is a real realm,

$$\log |\xi_s| = l_s(\xi);$$

and, if $\Omega^{(s)}$ and $\Omega^{(s')}$ are conjugate complex realms, put

$$\log(\xi_s) = \tfrac{1}{2} l_s(\xi) - i l_{s'}(\xi),$$
$$\log(\xi_{s'}) = \tfrac{1}{2} l_s(\xi) + i l_{s'}(\xi),$$
$$l_s(\xi) = \log(\xi_s) + \log(\xi_{s'}) = \log(\xi_s \xi_{s'}),$$

where $l_1(\xi), \cdots, l_n(\xi)$ are all real quantities. Observe that we may put

$$\xi_s = re^{-i\varphi + i2\pi k}, \qquad \xi_{s'} = re^{i\varphi - i2\pi k}, \qquad \xi_s \xi_{s'} = r^2,$$

and therefore from above

$$\log_s(\xi) = 2 \log r.$$

By definition we may take ξ_s and $\xi_{s'}$ such that $0 \leqq \varphi < 2\pi$, and that is

$$0 \leqq l_{s'}(\xi) < 2\pi.$$

The quantities $l_1(\xi), \cdots, l_n(\xi)$ are thus defined as one valued real functions of the quantities $u_1, \cdots, u_n$, and may be called the *logarithms for the form* ξ.

If further $lN(\xi)$ denotes the real part of the logarithm of $N(\xi)$, then is (since $r_1 + r_2 = r + 1$)

$$l_1(\xi) + \cdots + l_{r+1}(\xi) = lN(\xi).$$

If $u_1, \cdots, u_n$ are rational integers that do not all vanish, then is $\xi = \xi_1$ an algebraic integer, say α, in Ω.

The quantities $l_1(\xi), \cdots, l_n(\xi)$ are then uniquely determined through α and are called the *logarithms for the integer* α.

If ϵ is a unit in Ω then, since $N(\epsilon) = \pm 1$, it follows that

$$l_1(\epsilon) + l_2(\epsilon) + \cdots + l_{r+1}(\epsilon) = 0.$$

Observe that the real indeterminates $u_1, \cdots, u_n$ are *not* uniquely determined through the values of the logarithms $l_1(\xi), \cdots, l_m(\xi)$, being in fact 2^{r_1} valued, since the r_1 real values $\xi_1, \cdots, \xi_{r_1}$ are determined only as to sign, while the pairs of conjugate complex quantities $\xi_{r_1+1}, \cdots, \xi_n$ are completely determined.

ART. **139.** LEMMA. *In the realm* Ω *there is always a unit* ϵ *which satisfies the condition*

$$\gamma_1 l_1(\epsilon)+\cdots+\gamma_r l_r(\epsilon)\neq 0 \qquad (r+1=n),$$

where $\gamma_1, \cdots, \gamma_r$ *are arbitrarily prescribed real constants, which are not all zero.*

Proof. Let ω be any integer in Ω that is $\neq 0$, and for brevity put

$$L(\omega)=\gamma_1 l_1(\omega)+\cdots+\gamma_r l_r(\omega).$$

Further, determine any system of r real quantities $\lambda_1, \cdots, \lambda_r$, so that

$$\gamma_1\lambda_1+\cdots+\gamma_r\lambda_r=1,$$

and write

$$\Lambda_1=e^{\lambda_1 t}, \cdots, \Lambda_{r_1}=e^{\lambda_{r_1} t}, \Lambda_{r_1+1}=e^{\frac{1}{2}\lambda_{r_1+1} t}, \cdots, \Lambda_r=e^{\frac{1}{2}\lambda_r t},$$

where t is an arbitrary real parameter. Note that Λ_{r_1+1}, $\Lambda_{r_1+2}, \cdots$ occur, when there are imaginary realms.

There are two cases to consider: 1°, when all the n conjugate realms are real, and 2°, when some of them are conjugate complex.

In the first case, arrange according to the realms $\Omega^{(1)}, \cdots, \Omega^{(r)}$ the quantities $\Lambda_1, \cdots, \Lambda_r$ and for the last realm $\Omega^{(n)}(=\Omega^{(r+1)})$ put

$$\Lambda_n=\frac{|\sqrt{D}|}{\Lambda_1\cdots\Lambda_r}, \quad \text{so that therefore} \quad \Lambda_1\cdots\Lambda_n=|\sqrt{D}|.$$

In the second case corresponding to the r_1 real realms, again arrange the quantities $\Lambda_1, \cdots, \Lambda_{r_1}$; while corresponding to each complex pair $\Omega^{(r_1+1)}$ and $\Omega^{(r_1+r_2+1)}$; $\Omega^{(r_1+2)}$ and $\Omega^{(r_1+r_2+2)}$; $\cdots$, $\Omega^{(r_1+r_2)}$ and $\Omega^{(n)}$ arrange respectively the quantities $\Lambda_{r_1+1}, \Lambda_{r_1+2}, \cdots, \Lambda_r$; and finally, for the last of the conjugate complex pairs of realms $\Omega^{(r_1+r_2)}$ and $\Omega^{(n)}$ set down the value

$$\left|\left\{\frac{\sqrt{D}}{\Lambda_1\cdots\Lambda_{r_1}\Lambda_{r_1+1}\cdots\Lambda_n^2}\right\}^{\frac{1}{2}}\right|.$$

Again observe that $\Lambda_1\cdots\Lambda_n=|\sqrt{D}|$.

In both cases it is seen that the quantities $\Lambda_1, \cdots, \Lambda_n$ satisfy the requirements made of the constants $k_1, \cdots, k_n$ in the theorem of Art. 135.

Due to the theorem of Art. 135 there exists an integer α of Ω, which is different from zero, and is such that

$$|\alpha^{(1)}| \leqq \Lambda_1, \cdots, |\alpha^{(n)}| \leqq \Lambda_n, \tag{i}$$

and consequently $|N(\alpha)| \leqq |\sqrt{D}|$.

On the other hand, since $|N(\alpha)| \geqq 1$, it is clear that

$$|\alpha^{(s)}| \geqq \frac{1}{|\alpha^{(1)}| \cdots |\alpha^{(s-1)}| |\alpha^{(s+1)}| \cdots |\alpha^{(n)}|}.$$

Further since

$$\left|\frac{1}{\alpha^{(1)}}\right| \geqq \frac{1}{\Lambda_1}, \cdots, \left|\frac{1}{\alpha^{(n)}}\right| \geqq \frac{1}{\Lambda_n},$$

and as $\Lambda_1 \cdots \Lambda_n = |\sqrt{D}|$, it follows that

$$|\alpha^{(s)}| \geqq \frac{\Lambda_s}{|\sqrt{D}|}. \tag{ii}$$

From (ii) it is seen, if $\delta = \log|\sqrt{D}|$, that

$$2 \log|\alpha^{(s)}| \geqq 2 \log \Lambda_s - 2\delta,$$

which with (i) offer for imaginary complex pairs $\alpha^{(s)}$, $\alpha^{(s')}$ as well as for real α's the inequalities

$$\lambda_s t \geqq l_s(\alpha) \geqq \lambda_s t - 2\delta \qquad (s = 1, 2, \cdots, r),$$

2δ appearing with imaginary α's. From the latter expression it follows that the absolute value of $l_s(\alpha) - \lambda_s t$ lies between 0 and 2δ, or

$$0 \leqq |l_s(\alpha) - \lambda_s t| \leqq 2\delta \qquad (s = 1, 2, \cdots, r).$$

It is evident from this that the expression

$$\gamma_1\{l_1(\alpha) - \lambda_1 t\} + \cdots + \gamma_r\{l_1(\alpha) - \lambda_r t\} \equiv L(\alpha) - t$$

lies between two definite limits, say δ_1 and $\delta_2 > \delta_1$, which depend only upon D and $\gamma_1, \cdots, \gamma_r$, but not upon the parameter t.

From the inequality

$$\delta_1 < L(\alpha) - t < \delta_2,$$

it is seen that

$$\delta_1+t<L(\alpha)<\delta_2+t.$$

In this expression let t take successively the values 0, Δ, 2Δ, 3Δ, $\cdots$, where $\Delta=\delta_2-\delta_1+k$, k being a positive quantity. It is seen that

$$\begin{gathered}\delta_1<L(\alpha_0)<\delta_2,\\ \delta_2+k<L(\alpha_1)<2\delta_2-\delta_1+k,\\ 2\delta_2-\delta_1+2k<L(\alpha_3)<3\delta_2-2\delta_1+2k,\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\end{gathered}$$

where α_0, α_1, α_2, $\cdots$ are algebraic integers in Ω, whose norms are all less than $|\sqrt{D}|$, and which further satisfy the conditions

$$L(\alpha_0)<L(\alpha_1)<L(\alpha_2)<\cdots. \qquad \text{(iii)}$$

Observe that there are only a finite number of rational integers which in absolute value are less than $|\sqrt{D}|$. This finite number of rational integers can offer only a finite number of different ideal factors. Hence, among the infinite number of principal ideals (α_0), (α_1), (α_2), $\cdots$ there can appear only a finite number of different ideals. It follows that there is an indefinite number of such ideals that are equal.

If then $(\alpha)=(\beta)$, it is clear that α is divisible by (β) and that is, $\frac{\alpha}{\beta}$ and $\frac{\beta}{\alpha}$ are algebraic integers, or, $\epsilon=\frac{\beta}{\alpha}$ is an algebraic *unit*.

If β comes later in the series (iii) than α, then is

$$L(\epsilon)=L(\beta)-L(\alpha)>0,$$

which proves the lemma of this article.

ART. **140.** The lemma of the preceding article may be used to prove the fundamental theorem of Art. 122. For, let η be a unit in Ω for which $l_1(\eta_1)\neq 0$, and further

let η_2 be a unit for which

$$\gamma_1 = l_2(\eta_2) \qquad \text{and} \qquad -\gamma_2 = l_1(\eta_2),$$

where

$$\gamma_2 l_1(\eta_1) + \gamma_2 l_2(\eta_1) \neq 0,$$

or

$$\begin{vmatrix} l_1(\eta_1), & l_1(\eta_2) \\ l_2(\eta_1), & l_2(\eta_2) \end{vmatrix} \neq 0.$$

Then let η_3 be a unit for which

$$\begin{vmatrix} l_1(\eta_1), & l_1(\eta_2), & l_1(\eta_3) \\ l_2(\eta_1), & l_2(\eta_2), & l_2(\eta_3) \\ l_3(\eta_1), & l_3(\eta_2), & l_3(\eta_3) \end{vmatrix} \neq 0.$$

In this way derive a system of units $\eta_1, \cdots, \eta_r$, where finally the determinant

$$\begin{vmatrix} l_1(\eta_1), & \cdots, & l_1(\eta_r) \\ \cdots\cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots \\ l_r(\eta_1), & \cdots, & l_r(\eta_r) \end{vmatrix} \neq 0.$$

If H is any arbitrary unit of Ω, it is clear, due to the fact that the determinant just written is not zero, that real quantities $e_1, \cdots, e_r$ may be determined so that the r logarithms for H may be written in the form

$$\begin{aligned} l_1(H) &= e_1 l_1(\eta_1) + \cdots + e_r l_1(\eta_r), \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ l_r(H) &= e_1 l_r(\eta_1) + \cdots + e_r l_r(\eta_r). \end{aligned}$$

If m_1 is the greatest integer in e_1, m_2 in $e_2, \cdots, m_r$ in e_r, the above expressions may be written

$$\begin{aligned} l_1(H) &= m_1 l_1(\eta_1) + \cdots + m_r l_1(\eta_r) + E_1, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ l_r(H) &= m_1 l_r(\eta_1) + \cdots + m_r l_r(\eta_r) + E_r, \end{aligned}$$

where

$$\begin{aligned} E_1 &= \mu_1 l_1(\eta_1) + \cdots + \mu_r l_1(\eta_r) = l_1 \overline{H}, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ E_r &= \mu_1 l_r(\eta_1) + \cdots + \mu_r l_r(\eta_r) = l_r \overline{H}, \end{aligned}$$

where the quantities $\mu_1, \cdots, \mu_r$ are real and $\geqq 0$ and <1.

It is clear that the values $E_1, \cdots, E_r$ are in absolute value less than a fixed quantity k, which does *not* depend upon H.

Observing that

$$\overline{H} = \frac{H}{\eta_1^{m_1} \cdots \eta_r^{m_r}}$$

is a *reduced unit*, it is seen that the r logarithms for H are in absolute value less than k.

Since (see Art. 138)

$$l_1(\overline{H}) + \cdots + l_{r+1}(\overline{H}) = 0,$$

it is clear that the absolute value of $l_{r+1}(\overline{H})$ is less than kr. There consequently exist the inequalities

$$|\overline{H}^{(1)}| < e^k, \cdots, |\overline{H}^{(r)}| < e^k, |\overline{H}^{(r+1)}| < e^{rk};$$

and that is, all the conjugate values of the unit $\overline{H}$ are in absolute value less than e^{rk}.

Due to a theorem in Art. 135 there are only a finite number of such units. Denote them by $H_1, \cdots, H_G$. It follows that $\overline{H} = H_S$, and accordingly,

$$H = H_S \eta_1^{m_1} \cdots \eta_r^{m_r},$$

where S has one of the values $1, \cdots, G$. Hence, if H_T is any one of the units $H_1, \cdots, H_G$, and if we form the first $G+1$ powers of H_T, it follows that there must be two of these powers which are expressed in the form

$$H_S \eta_1^{m_1'} \cdots \eta_r^{m_r'} \quad \text{and} \quad H_S \eta_1^{m_1''} \cdots \eta_r^{m_r''}.$$

It is seen that the quotient of these two units has the form $\eta_1^{m_1} \cdots \eta_r^{m_r}$. It is thus proved that for each of the units $H_1, \cdots, H_G$, say $H_T (T = 1, 2, \cdots, G)$ there exists an exponent M_T such that $H_T^{M_T}$ is equal to a product of powers of $\eta_1, \cdots, \eta_r$. If the least common multiple of $M_1, \cdots, M_G$ is denoted by M, it is clear that each of the reduced units $H_1, \cdots, H_G$ has the property that H_T^M is

equal to a product of powers of $\eta_1, \eta_2, \cdots, \eta_r$. From this it follows that the r logarithms for any arbitrary unit H of the realm Ω may be expressed in the form

$$(1)\qquad \begin{cases} l_1(H) = \dfrac{m_1 l_1(\eta_1) + \cdots + m_r l_1(\eta_r)}{M}, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ l_r(H) = \dfrac{m_1 l_r(\eta_1) + \cdots + m_r l_r(\eta_r)}{M}, \end{cases}$$

where $m_1, \cdots, m_r$ are rational integers.

ART. 141. If next we consider all the units of Ω, and for each unit form a corresponding system of logarithms as in (1) above and if we proceed with these systems of logarithms as was done in detail in Vol. I, Art. 96 for the determination of a basis for all integers of Ω, it is seen that there exists a system of r units, say $\epsilon_1, \cdots, \epsilon_r$, such that through the logarithms of these r units the logarithms for every arbitrary unit H of the realm Ω may be expressed in the form

$$(2)\qquad l_i(H) = a_1 l_i(\epsilon_1) + \cdots + a_r l_i(\epsilon_r) \quad (i = 1, 2, \cdots, r),$$

where $a_1, \cdots, a_r$ are rational integers. This system of units $\epsilon_1, \cdots, \epsilon_r$ fulfill the requirements demanded in the Dirichlet Theorem of Art. 130.

In fact, if H is an arbitrary unit and if the logarithms for it have the form just written, then

$$(3)\qquad \rho = \frac{H}{\epsilon_1^{a_1} \cdots \epsilon_r^{a_r}},$$

is a unit *reduced with respect to* H. The logarithms for ρ are all $=0$. Such a unit is necessarily a root of unit. For, from what was proved above

$$\rho^M = \eta_1^{m_1} \cdots \eta_r^{m_r},$$

where $m_1, \cdots, m_r$ are rational integers. Taking the logarithm of this expression and observing from (3)

that $\log \rho = 0$, it is seen that

$$\begin{aligned} m_1 l_1(\eta_1) + \cdots + m_r l_1(\eta_r) &= 0, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & \\ m_1 l_r(\eta_1) + \cdots + m_r l_r(\eta_r) &= 0. \end{aligned}$$

It follows that

$$m_1 = 0, \ \cdots, \ m_r = 0,$$

and consequently,

$$\rho^M = 1.$$

From this follows at once the expression of H in (3) in the form required by Dirichlet's Theorem.

From the method in which $\epsilon_1, \cdots, \epsilon_r$ were determined, it is clear that

$$\begin{vmatrix} l_1(\eta_1), & \cdots, & l_1(\eta_r) \\ \cdots\cdots & & \cdots\cdots \\ l_r(\eta_1), & \cdots, & l_r(\eta_r) \end{vmatrix} = A \begin{vmatrix} l_1(\epsilon_1), & \cdots, & l_1(\epsilon_r) \\ \cdots\cdots & & \cdots\cdots \\ l_r(\epsilon_1), & \cdots, & l_r(\epsilon_r) \end{vmatrix} = A \cdot R,$$

where A is a determinant which is a rational integer, varying with every system of independent units $\eta_1, \cdots, \eta_r$ and where the determinant R is the regulator of the realm Ω, an invariantive quantity $\neq 0$. The sequence of the units $\epsilon_1, \cdots, \epsilon_r$ must be so taken that R is positive. From this it is clear that the expression of the unit H through the units $\epsilon_1, \cdots, \epsilon_r$ may be done in only *one* way. The proof of the Theorem of Art. 138 is thus completed in all detail.

The above proof of Dirichlet's Theorem also offers a means (difficult though it be) of determining the system of units $\epsilon_1, \cdots, \epsilon_r$ through a finite number of operations. A method of treating this question leads to a Theory of the Algorithms in continued fractions which with the allied questions of periodicity is treated by Minkowski. ("Généralization de la théorie des fractions continués," *Ann. de l'École Normale*, 1896, 3^{d} Série, t. XIII; *Collected Works*, Vol. I, p. 278.)

ART. **142. The Fundamental Units.** The system of units $\epsilon_1, \cdots, \epsilon_r$, that was introduced in the previous article, was called (Art. 127) a system of *fundamental units of the realm* Ω.

It is clear, if $\eta_1, \cdots, \eta_r$ is another system of fundamental units, that the determinant of the corresponding system of the r logarithms must be the same as R except as to sign. For

$$\begin{vmatrix} l_1(\eta_1), & \cdots, & l_1(\eta_r) \\ \cdots\cdots & & \cdots\cdots \\ \cdots\cdots & & \cdots\cdots \\ l_r(\eta_1), & \cdots, & l_r(\eta_r) \end{vmatrix} = A \begin{vmatrix} l_1(\epsilon_1), & \cdots, & l_1(\epsilon_r) \\ \cdots\cdots & & \cdots\cdots \\ \cdots\cdots & & \cdots\cdots \\ l_r(\epsilon_1), & \cdots, & l_r(\epsilon_r) \end{vmatrix}$$

$$= AA_1 \begin{vmatrix} l_1(\eta_1), & \cdots, & l_1(\eta_r) \\ \cdots\cdots & & \cdots\cdots \\ \cdots\cdots & & \cdots\cdots \\ l_r(\eta_1), & \cdots, & l_r(\eta_r) \end{vmatrix},$$

so that $AA_1 = 1$, or $A = A_1 = \pm 1$.

In the proof of the results of the preceding article, it was seen that a unit whose corresponding logarithms were all $= 0$, was necessarily a root of unity. And this has expression in the following.

THEOREM. *Every unit, which with all its conjugates are in absolute value equal to 1, is a root of unity.*

Direct proofs of this theorem are given by Kronecker, *Werke*, Vol. I, p. 103, and by Minkowski, paper above noted in the *Ann. de l'École Normale*, and *Geometrie der Zahlen*, § 43. Also note proof given by Weber, *Alg.*, Vol. II, p. 705.

Since -1 and 1 are roots of unity in every algebraic realm, and since every other root of unity is a complex quantity, it is seen that the number of all roots of unity in any realm is even and that this number is only greater than 2 when all the conjugate realms are imaginary.

ART. **143.** An arbitrary system of t units $\eta_1, \cdots, \eta_t$ is called a *system* of t *independent* units, if among them

there exists no equation of the form

$$\eta_1^{m_1} \cdots \eta_t^{m_t} = 1,$$

where $m_1, \cdots, m_t$ are rational integers. The number t must (Art. 140) always be $\leqq r$. In particular, the system of fundamental units $\epsilon_1, \cdots, \epsilon_r$ forms a system of r independent units.

If there exists another system of r independent units $\eta_1, \cdots, \eta_r$, an integer M may always be found, such that for every unit ϵ of Ω there is an equation of the form

$$\epsilon^M = \eta_1^{m_1} \cdots \eta_r^{m_r},$$

where $m_1, \cdots, m_r$ are rational integers. For, by Dirichlet's Theorem

$$(2) \qquad \eta_s = \rho_s \epsilon_1^{a_{1s}} \cdots \epsilon_r^{a_{rs}} \qquad \text{for} \qquad s = 1, 2, \cdots, r,$$

where ρ is a definite root of unity for each s, and $a_{1s}, \cdots, a_{rs}$ are rational integers. Further, the determinant $\sum \pm a_{11} \cdots a_{rr}$ is different from zero due to the fact that the η's are independent units. Denote this determinant by A. It follows from (2), if

$$\frac{\eta_s}{\rho_s} = \bar{\eta}_s,$$

that

$$\log(\bar{\eta}_s) = a_{1s} \log(\epsilon_1) + \cdots + a_{rs} \log(\epsilon_r) \qquad (s = 1, 2, \cdots, r).$$

Hence,

$$\log(\epsilon_t) = \frac{1}{A}[A_{1t} \log(\bar{\eta}_1) + \cdots + A_{rt} \log(\bar{\eta}_r)] \qquad (t = 1, 2, \cdots, r),$$

where the A's are rational integers, or

$$\epsilon_t \rho_1^{\frac{A_{1t}}{A}} \cdots \rho_r^{\frac{A_{rt}}{A}} = \eta_1^{\frac{A_{1t}}{A}} \cdots \eta_r^{\frac{A_{rt}}{A}} \qquad (t = 1, 2, \cdots, r).$$

By the Dirichlet Theorem $\epsilon = \rho \epsilon_1^{a_1} \cdots \epsilon_r^{a_r}$ and, if $\rho^E = 1$ for all the roots of unity in the fixed realm, then clearly the integer $M = AE$ has the property required of M above.

CHAPTER VIII

EXTRACTS FROM MINKOWSKI'S GEOMETRY OF NUMBERS

ART. **144.** Let $x_1, x_2, \cdots, x_n$ be a system of real quantities independent of one another, which are continuous and may have infinite values. These quantities may be taken as the rectangular coördinates of a point in space S_n of n dimensions. We thus have a mode of expression which is visualized in the cases $n=1$, 2, 3 and which through analogy is at once intelligible in the general case. It is seen that the results derived in the general case may be checked as to correctness by making $n=1$, 2, 3, and by noting the corresponding results in these cases. Accordingly, in S_n we shall speak of a point x which may be represented by a system of real values $x_1, x_2, \cdots, x_n$. These vary in a continuous manner as x is caused to move in a continuous manner. If y is a second point in S_n with coördinates $y_1, y_2, \cdots, y_n$, the positive square root

$$(1) \qquad \rho = \sqrt{(x_1-y_1)^2+(x_2-y_2)^2+\cdots+(x_n-y_n)^2}$$

denotes the *distance* between the two points. The totality (or collectivity) of all points y, whose distance from x does not exceed a definite positive quantity ϵ, where ϵ is taken arbitrarily small, is called the *neighborhood* of the point x.

We consider next a domain X of points in S_n, regarding which the two following postulates are made:

I. With respect to each point in S_n it is definitely determined whether or not it belongs to X.

II. X is finite; that is, the coördinates of every point x in X are contained between definite finite limits.

A point having a neighborhood, in which all the points belong to X, is called an *interior* point of X. A point, in whose neighborhood no point of X is situated, is called an *exterior* point of X.

A point in whose neighborhood are situated points that belong to X and points that do not belong to X is called a *boundary point* of X. The totality of all boundary points is called the *boundary* of X and is denoted by B.

The interior points belong to the domain X, the exterior points do *not* belong to this domain. We shall consider (although it is unessential) the boundary points as belonging to X.

The collectivity of all points whose coördinates satisfy a linear equation is called a *plane*. The *coördinate* planes are

$$x_i = 0 \qquad (i = 1, 2, \cdots, n).$$

The space S_n is divided by means of n equidistant assemblages of planes which are parallel to the coördinate planes

$$\cdots,\ x_i = a_i - \delta,\ x_i = a_i,\ x_i = a_i + \delta,\ x_i = a_i + 2\delta,\ \cdots \qquad (i = 1, 2, \cdots, n)$$

into elements, called cuboids or *cells* (*Würfeln*). In two dimensions these cells are squares and they are cubes in three dimensions. The volume of a cell is δ^n.

The *interior* of a cell is determined through the n inequalities

$$a_i + k_i\delta < x_i < a_i + (k_i + 1)\delta \qquad (i = 1, 2, \cdots, n),$$

where the k's are integers.

Among these cells there are some which contain only points of X and which may therefore be called *interior*

cells. There are a finite number of them. Denote this number by M.

Among the cells there are others which contain points of X and also points that do not belong to X. These may be called *boundary* cells. Denote this number by m.

If there exist boundary cells, it is evident that the volume $M\delta^n$ does not contain all the points of X. However, $(M+m)\delta^n$ does contain all the points of X and in addition other points. We may therefore say that the volume V of X lies between the limits

$$M\delta^n \leqq V \leqq (m+M)\delta^n. \tag{2}$$

Now, if δ is diminished in a continuous manner, the numbers M and m become larger and larger and in such a way that $M\delta^n$ increases while $(M+m)\delta^n$ decreases. These two quantities are finite and approach definite limits. If the two limits are the same, it is evident that

$$\lim M\delta^n = \lim (m+M)\delta^n = V; \tag{3}$$

or, if

$$\lim m\delta^n = 0, \tag{4}$$

then V may be called the *volume* of X. When this condition is satisfied, the limiting value[1] of V is the same if other methods of distribution of the elementary parallelopipedons are introduced, where the domain is distributed into elements through surfaces that have been formed otherwise.

Each of the elementary cells in the space S_n has a definite center. Let N denote the number of centers which lie within the domain X. Hence, since every interior cell has its center within X and since every exterior cell has its center on the outside of X, it follows that

$$M \leqq N \leqq M+m.$$

[1] See Riemann's *Works*, No. 12, and for the extension to multiple integrals see Wilson's *Advanced Calculus*, pp. 50 ff.

Hence,

$$N\delta^n - m\delta^n \leqq M\delta^n, \qquad \text{and} \qquad (M+m)\delta^n \leqq N\delta^n + m\delta^n.$$

It therefore follows from (2) that

$$N\delta^n - m\delta^n \leqq V \leqq N\delta^n + m\delta^n.$$

If we put

$$V = N\delta^n + R\delta,$$

then it is seen that

$$-m\delta^{n-1} < R < m\delta^{n-1}.$$

It may be proved as follows that $m\delta^{n-1}$ lies within a finite limit, so that $m\delta^n$ approaches zero when δ is very small. Suppose that the boundary B of X consists of a finite number of portions $B_1, B_2, \cdots$, in each of which one of the coördinates of the point x may be expressed as a one-valued and continuous function of the others. For example, in B_i let

$$x_n = \varphi(x_1, x_2, \cdots, x_{n-1}).$$

(Compare this with a volume and a surface in three dimensional space.) The values of $x_1, x_2, \cdots, x_{n-1}$ which appear in B_i fill a domain X_{n-1} in an $n-1$ dimensional space S_{n-1} which may be called the projection of B_i. A cell which within its interior contains points of B_i is said to be *cut* by the surface B_i. Let c be such a cell, whose number, say, is m_i. Then the coördinates $x_1, x_2, \cdots, x_{n-1}$ which correspond to points of c fill an $n-1$ dimensional cell c' whose volume is δ^{n-1}. Let M' be the number of the cells c'. If the number of cells c which are projected into an $n-1$ cell c' does not exceed a finite number a (and that is, if there are only a finite number of cells of the nth dimension that are cut by B_i and which are projected on one cell of the $(n-1)$th dimension),[1] then is

$$m_i\delta^{n-1} \leqq aM'\delta^{n-1}.$$

[1] This assumption is further considered by Weber, *Algebra* II, p. 676.

Evidently the quantity $M'\delta^{n-1}$ is less than the volume of an $n-1$ dimensional cell C that is taken so great that the entire domain X_{n-1} lies within it. Consequently, it follows that

$$m_i\delta^{n-1} < aC;$$

and that is, $m_i\delta^{n-1}$ is less than a definite finite value however small δ is taken.

The above may be formulated in the theorem.

THEOREM. *If V is the volume of the domain X and if N is the number of centers of cells, which centers lie within X, then is*

$$V = N\delta^n + R\delta,$$

where R is a quantity which, however small δ may be, in absolute value does not exceed a finite limit.

It follows that

$$V = \lim_{\delta \to 0} N\delta^n.$$

ART. **145. The Computation of the Volume.** Let $u_1, u_2, \cdots, u_n$ be continuous functions of the variables $x_1, x_2, \cdots, x_n$ in the domain X and such that to every point in X there corresponds a system of values of the variables u; and reciprocally to every system of values of the variables u in a certain domain U there corresponds a point in X. Thus to the domain X there corresponds the domain U in a space S_n in which the u's are the coördinates.

The functional determinant

$$\sum \pm \frac{\partial x_1}{\partial u_1}\frac{\partial x_2}{\partial u_2}\cdots\frac{\partial x_n}{\partial u_n}$$

which occurs in this transformation was called by Sylvester after Jacobi,[1] the *Jacobian* of the functions $x_1, x_2, \cdots, x_n$ with respect to the variables $u_1, u_2, \cdots, u_n$ and

[1] Jacobi, "De determinantibus functionalibus," *Crelle*, Vol. 22, 1841; *Werke*, Vol. 3, pp. 392 ff.

may be denoted by the symbol

$$\frac{d(x_1, x_2, \cdots, x_n)}{d(u_1, u_2, \cdots, u_n)}.$$

The properties of the Jacobian are given in the text books on determinants. See for example Chapt. XIII of Scott and Mathews, *Theory of Determinants;* Weber, *Algebra*, Vol. II, p. 680.

In particular, it is seen that

$$(1)\quad \frac{d(x_1, x_2, \cdots, x_n)}{d(v_1, v_2, \cdots, v_n)} = \frac{d(x_1, x_2, \cdots, x_n)}{d(u_1, u_2, \cdots, u_n)} \frac{d(u_1, u_2, \cdots, u_n)}{d(v_1, v_2, \cdots, v_n)},$$

where $u_1, u_2, u_3, \cdots, u_n$ are functions of the new variables $v_1, v_2, \cdots, v_n$.

We further have

$$(2)\quad \frac{d(x_1, x_2, \cdots, x_n)}{d(u_1, u_2, \cdots, u_n)} = \frac{1}{\dfrac{d(u_1, u_2, \cdots, u_n)}{d(x_1, x_2, \cdots, x_n)}}.$$

If the functional determinant in the domains X or V is not infinite, there exists the transformation [1]

$$V = \int \cdots \int\int dx_1 dx_2 \cdots dx_n$$
$$= \int \cdots \int\int \frac{d(x_1, x_2, \cdots, x_n)}{d(u_1, u_2, \cdots, u_n)} du_1 du \cdots du_n,$$

where the first integral is to be taken over the domain X, while the second integral is to be given a positive value, if the elements of integration $dx_1, dx_2, \cdots, dx_n$ and $du_1, du_2, \cdots, du_n$ are taken positive.

To apply the above transformations, let $y_1, y_2, \cdots, y_n$ be a system of independent linear functions of $x_1, x_2, \cdots, x_n$ expressed through the relations

$$(3)\quad y_i = c_{1i}x_1 + c_{2i}x_2 + \cdots + c_{ni}x_n \quad (i=1, 2, \cdots, n);$$

and assume that the y's are either all real or, if there

[1] See Wilson's *Advanced Calculus*, p. 336.

appear imaginary y's, that also their conjugates are to be found among the above relations.

It is seen that the determinant

$$D=\sum\pm c_{11}c_{22}\cdots c_{nn}$$

is either real, or, if the number of pairs of conjugate y's is odd, the determinant is a pure imaginary.

Denote the real y's by $y_1, y_2, \cdots, y_s$, while $(y_{s+1}, y_{\nu+1})$, $(y_{s+2}, y_{\nu+2})$, $\cdots$, (y_ν, y_n) indicate the imaginary pairs which are in number $\nu-s=n-\nu$, so that

$$s=2\nu-n.$$

Let $r_1, r_2, \cdots, r_\nu$ denote real quantities and put

$$y_1=r_1,\ y_2=r_2,\ \cdots,\ y_s=r_s;$$
$$y_{s+1}=r_{s+1}e^{i\varphi_1},\ \cdots,\ y_\nu=r_\nu e^{i\varphi_{n-\nu}};$$
$$y_{\nu+1}=r_{s+1}e^{-i\varphi_1},\ \cdots,\ y_n=r_\nu e^{-i\varphi_{n-\nu}}.$$

In this scheme $r_1, r_2, \cdots, r_s$ are to be unrestricted so long as the x's are unrestricted, while the quantities $r_{s+1}, r_{s+2}, \cdots, r_\nu$ are to take *only positive values* (including zero), the angles $\varphi_1, \varphi_2, \cdots, \varphi_{n-\nu}$ being restricted to the intervals

$$0\leqq\varphi_1<2\pi,\ \cdots,\ 0\leqq\varphi_{n-\nu}<2\pi.$$

Through this convention it is seen that to every point x there will correspond a definite system of values $r_1, r_2, \cdots, r_\nu, \varphi_1, \varphi_2, \cdots, \varphi_{n-\nu}$ and *vice versa*.

Further, observe that

$$\frac{d(x_1, x_2, \cdots, x_n)}{d(r_1, r_2, \cdots, r_\nu, \varphi_1, \varphi_2, \cdots, \varphi_{n-\nu})}$$
$$=\frac{d(x_1, x_2, \cdots, x_n)}{d(y_1, y_2, \cdots, y_n)}\,\frac{d(y_1, y_2, \cdots, y_n)}{d(r_1, \cdots, r_\nu, \varphi_1, \cdots, \varphi_{n-\nu})}$$
$$=\frac{1}{D}\,\frac{d(y_{s+1}, y_{\nu+1})}{d(r_{s+1}, \varphi_1)}\cdots\frac{d(y_\nu, y_n)}{d(r_\nu, \varphi_{n-\nu})};$$

and since

$$\frac{d(y_{s+1}, y_{\nu+1})}{d(r_{s+1}, \varphi_1)}=\frac{\partial y_{s+1}}{\partial r_{s+1}}\frac{\partial y_{\nu+1}}{\partial \varphi_1}-\frac{\partial y_{\nu+1}}{\partial r_{s+1}}\frac{\partial y_{s+1}}{\partial \varphi_1}=-2ir_{s+1}, \text{ etc.},$$

it follows that

$$\frac{d(x_1, x_2, \cdots, x_n)}{d(r_1, \cdots, r_\nu, \varphi_1, \cdots, \varphi_{n-\nu})} = \frac{(-2i)^{n-\nu}}{D} r_{s+1} r_{s+2} \cdots r_\nu.$$

As there are $n-\nu$ pairs of imaginary roots found in D, each pair contributing an i, the factor $\frac{(-2i)^{n-\nu}}{D}$ is a real quantity; and, if the absolute value of D is denoted by Δ, it follows that

$$V = \frac{2^{n-\nu}}{\Delta} \int \cdots \int\int dr_1 \cdots dr_s r_{s+1} dr_{s+1} \cdots r_\nu dr_\nu d\varphi_1 \cdots d\varphi_{n-\nu}.$$

If the domain Y of the y's is such that only the absolute values of the linear functions in (3) appear, the value of V just given may be further simplified. In this case corresponding to any system of values of the variables $r_1, r_2, \cdots, r_\nu$, there correspond *all* the values of $\varphi_1, \varphi_2, \cdots, \varphi_{n-\nu}$, which satisfy the conditions

$$0 \leqq \varphi_1 < 2\pi, \cdots, 0 \leqq \varphi_{n-\nu} < 2\pi.$$

The formula for V becomes

$$V = \frac{(4\pi)^{n-\nu}}{\Delta} \int \cdots \int\int r_{s+1} \cdots r_\nu dr_1 dr_2 \cdots dr_\nu.$$

Further, observe under the same conditions that a definite system of values of the quantities $r_2, r_3, \cdots, r_\nu$ corresponds to every value of r_1 there corresponds also the opposite value, so that

$$\int_{-a_1}^{a_1} = \int_0^{a_1} + \int_{-a_1}^{0}.$$

Hence, the integral with respect to r_1 may be distributed into two parts, in the one of which r_1 is positive and in the other negative. If this distribution is made for all the real y's in the scheme (3), and if we observe that

$$2n - 2\nu + s = 2n - 2\nu + 2\nu - n = n,$$

it is seen that

$$(4) \qquad V=\frac{2^n\pi^{n-\nu}}{\Delta}\int\cdots\int\int r_{s+1}\cdots r_\nu dr_1 dr_2\cdots dr_\nu,$$

where now the variables $r_1, r_2, \cdots, r_\nu$ are all limited to positive values.

ART. 146. **The Functions $S(a, b)$ and $E(a, b)$.** Denote the points in the n-dimensional space S_n by the letters $a, b, \cdots, x, \cdots$, where the coördinates of a are $a_1, a_2, \cdots, a_n$, the coördinates of b being $b_1, b_2, \cdots, b_n$, etc.

A function of the coördinates $a_1, a_2, \cdots, a_n$ is called a function of the point a and may be denoted by $f(a)$.

Similarly, a function of two points a and b, may be denoted by $f(a, b)$, etc.

Among the points of S_n those, whose coördinates are integers, are particularly noteworthy. These points are called *lattice-points* in S_n. They lie upon n assemblages of equivalent parallel planes, which divide the space S_n into cells (Art. 144). Each of these cells has the volume 1.

Consider a function $S(a, b)$ of two points[1] which satisfies the postulates:

I. $S(a, b)$ is for any two points a and b that are different from each other, positive and finite and vanishes only if a and b coincide.

II. If a, b, c, d are four points $(a \neq b)$, which four points are so situated that a positive value of t may be determined such that

$$a_i - b_i = t(c_i - d_i),$$

then is $S(a, b) = tS(c, d)$. Geometrically interpreted, this postulate means that the lengths (ab) and (cd) are parallel and are to each other as $t : 1$. Analytically, the formula signifies *here* that S is a homogeneous function of the first degree in the differences $a_i - b_i$.

[1] Weber's *Algebra*, Vol. II, p. 681.

III. If a, b, c are any three points, then is

$$S(a, c) \leqq S(a, b) + S(b, c).$$

IV. $S(a, b) = S(b, a)$.

Functions which satisfy the above postulates were called by Minkowski interchangeable, concurrent line-distances, or in general, *line-distances*. As the terminology is somewhat of a misnomer, it will not be used.

If O is the center of coördinates and if $x_i = a_i - b_i$, it follows from III that

$$S(o, x) = S(a, b) = S(x),$$

say, so that $S(a, b)$ is expressed as a function of the one point x.

$E(a, b)$ may be defined as the half-side of a cell whose edges are parallel to the coördinate axes and whose center is at a, the point b being on the surface of the cell. In other words $E(a, b)$ is the greatest of the absolute values of the n differences $a_i - b_i$.

From the inequality

$$|a_i - c_i| = |a_i - b_i + b_i - c_i| \leqq |a_i - b_i| + |b_i - c_i|,$$

it follows that

$$E(a, c) \leqq E(a, b) + E(b, c).$$

Accordingly, $E(a, b)$ satisfies the four postulates required of the function $S(a, b)$.

All points x which satisfy the condition

$$E(o, x) = E(x) = 1$$

lie upon the surface of a cell whose center is at the origin, and the length of the sides is 2.

If $S(a, b)$ is any function that satisfies the four postulates made at the beginning of this article, then the values, which the function $S(x)$ takes for the points of this cell-surface, have an upper limit K and a lower limit k. Due to the postulate II the ratio $S(x) : E(x)$ depends only upon the ratios of the coördinates $x_1 : x_2 : \cdots : x_n$.

It is evident that for any point x of the cell there exists the inequalities

$$kE(x) \leqq S(x) \leqq KE(x);$$

and hence from postulate II

$$kE(x) \leqq S(x) \leqq KE(x) \tag{i}$$

for any point whatever.

Let a be any lattice-point and observe that all points which satisfy the condition

$$E(x) = \frac{S(a)}{k} \tag{ii}$$

lie upon the surface of a cell whose center is at the origin.

If y is a point without this cell, then is

$$E(y) > \frac{S(a)}{k}. \tag{iii}$$

In the cell determined through (ii) including the surface of this cell, there lies at least one lattice-point, namely a. Evidently, there are only a finite number of lattice-points in such a cell. Among the values which $S(x)$ takes for these lattice-points there is one which has the least value; and, if this smallest value exists for the lattice-point c, then is

$$S(c) \leqq S(a). \tag{iv}$$

For any point c' situated without the cell, it is evident from (ii) that

$$kE(c') > S(a).$$

Hence, due to (iv) and (i),

$$S(c') > S(c).$$

It is thus proved that $S(c)$ is the minimum among all the values which the function $S(x)$ can have for any lattice-point that is different from zero. It is also evident that $S(c)$ is the minimum among all the values of the function $S(a, b)$ for two different lattice-points a and

b. This value which may be denoted by M is called the *minimum of the function S*.

Observe that upon the cell $E(x)=1$, there are certain lattice-points for example $x_1=1,\ x_2=0,\ x_3=0,\ \cdots,\ x_n=0$. Hence, due to the significance of K and the formula (i),

$$M \leqq K,$$

so that there is an upper limit of M.

If h is a constant, all points which satisfy the condition

$$S(x) \leqq h \qquad \text{(v)}$$

fill a finite portion of space, say S, which has a definite volume. Denote by J the volume of the portion of space S_0 which is determined through

$$S(x) \leqq 1.$$

Hence, the volume of the portion of space S is equal to $h^n J$. From (i) it appears that all points which satisfy the condition (v) also satisfy the inequality

$$E(x) \leqq \frac{h}{k}. \qquad \text{(vi)}$$

Accordingly, the portion of space S lies wholly in the cell that is determined through (vi). The volume of this cell is $\frac{h^n}{k^n}$ which quantity is therefore an upper limit for the volume of J.

If next a and b are any two lattice-points, the two portions of space A and B which are determined through

$$S(a, x) \leqq \tfrac{1}{2}M, \qquad S(b, x) \leqq \tfrac{1}{2}M \qquad \text{(vii)}$$

have either no points in common or at most only portions of their surface. For, if x is an arbitrary point, then due to the postulate III, above,

$$S(a, b) \leqq S(a, x) + S(b, x);$$

and due to the significance of M, the quantity $S(a, b)$ is

not smaller than M. Hence we must have

$$M \leqq S(a, x) + S(b, x).$$

This is in accord with (vii), only when

$$S(a, x) = \tfrac{1}{2}M = S(b, x).$$

Now let m be any rational integer and consider the lattice-points whose coördinates are any of the integers $0, \pm 1, \pm 2, \cdots, \pm m$. The number of such points is $(2m+1)^n$ and they all lie in a cell whose edges are $2m$ in length. About each of these lattice-points a construct the portion of space A which is defined through

$$S(a, x) \leqq \tfrac{1}{2}M,$$

and whose volume is equal to $(\frac{1}{2}M)^n J$. These portions of space are all contained in a cell whose center is at the origin and whose edges are in length (see (vi)) equal to

$$2m + \frac{M}{k}.$$

As was seen above, the portions of space A do not overlap one another, so that their combined volume is not greater than the volume of the cell which encloses them, and that is,

$$(2m+1)^n (\tfrac{1}{2}M)^n J \leqq \left(2m + \frac{M}{k}\right)^n.$$

In this expression m may be allowed to increase indefinitely with the resulting fundamental equation

$$(\tfrac{1}{2}M)^n J \leqq 1. \qquad \text{(vii)}$$

The determination of J in this expression may be often made through an integration.

The following cases may serve not only as examples, but they are important on account of later applications.[1]

[1] See Weber's *Lehrbuch der Algebra*, Vol. II, p. 685, which has been followed closely in the presentation of this chapter, the results being taken from Minkowski's *Geometrie der Zahlen*.

ART. **147.** EXAMPLE 1. (See Minkowski, *Geometrie der Zahlen*, p. 102.)

Let $y_1, y_2, \cdots, y_n$ be a system of linear functions of $x_1, x_2, \cdots, x_n$ defined through the equations

$$y_k = \sum_{i=1}^{i=n} A_{ik} x_i \qquad (k=1, 2, \cdots, n),$$

where the A_{ik} are real quantities, whose determinant

$$\pm\Delta = \sum \pm A_{11} A_{22} \cdots A_{nn}$$

is different from zero.

Define the function $S(a, b)$ as the greatest among the absolute values of the n functions

$$\sum_{i=1}^{i=n} A_{ik}(a_i - b_i) \qquad (k=1, 2, \cdots, n).$$

It is at once evident that this function satisfies postulates I, II and IV of Art. 146. Observe further that the postulate III is satisfied. For, by definition, $S(a, c)$ is the smallest number which for $k=1, 2, \cdots, n$ satisfies the inequalities

$$\left| \sum_{i=1}^{i=n} A_{ik}(a_i - c_i) \right| \leqq S(a, c). \qquad \text{(i)}$$

On the other hand for every k we have

$$\left| \sum_{i=1}^{i=n} A_{ik}(a_i - c_i) \right| \leqq |\sum A_{ik}(a_i - b_i)| + |\sum A_{ik}(b_i - c_i)|;$$

and consequently

$$\left| \sum_{i=1}^{i=n} A_{ik}(a_i - c_i) \right| \leqq S(a, b) + S(b, c).$$

It follows from (i) that

$$S(a, c) \leqq S(a, b) + S(b, c).$$

The points which satisfy the equation $S(x) = 1$ form the boundary of a portion of space. The points of this portion of space satisfy the inequality

$$-1 \leqq y_i \leqq +1.$$

The volume of this portion of space is

$$J = \int \cdots \int \int dx_1 dx_2 \cdots dx_n$$

$$= \int \cdots \int \int \frac{d(x_1, x_2, \cdots, x_n)}{d(y_1, y_2, \cdots, y_n)} dy_1 dy_2 \cdots dy_n$$

$$= \frac{1}{\Delta} \int_{-1}^{+1} \cdots \int_{-1}^{+1} \int_{-1}^{+1} dy_1 dy_2 \cdots dy_n = \frac{2^n}{\Delta}.$$

Hence, from formula (vii) of the preceding article,

$$M \leqq \sqrt[n]{\Delta}.$$

The expression of this theorem as given by Minkowski is:

In every system of n real linear functions of n variables with a determinant $\pm\Delta$, *which does not vanish, integral values that are not all zero may always be given to the variables such that none of the absolute values of these functions is greater than* $\sqrt[n]{\Delta}$.

Other proofs of this theorem are found in Vol. I, Arts. 26 ff.

ART. 148. EXAMPLE 2. As in Art. 147 let $y_1, y_2, \cdots, y_n$ be a system of independent linear functions of $x_1, x_2, \cdots, x_n$, whose determinant has the absolute value Δ. Of these y's let there be $n-\nu$ pairs of imaginary and $s = 2\nu - n$ real functions; and further, let

$$S(x) = |y_1| + |y_2| + \cdots + |y_n|.$$

If $\alpha_i, \beta_i, \gamma_i$ are the values of the function y_i at the points a, b, c, then is

$$S(a, b) = |\sum(\alpha_i - \beta_i)|;$$

and since the absolute value of a sum is never greater than the sum of the absolute values, it is seen that

$$|\sum(\alpha_i - \nu_i)| \leqq |\sum(\alpha_i - \beta_i)| + |\sum(\beta_i - \nu_i)|.$$

It is thus shown that the four postulates of Art. 146 are satisfied.

Due to the definition of J in Art. 146, it is seen that

$$J=\frac{2^n\pi^{n-\nu}}{\Delta}\int\int\cdots\int r_{s+1}\cdots r_\nu dr_1\cdots dr_\nu,$$

where the integration is to be taken over all positive values of $r_1, r_2, \cdots, r_\nu$ which satisfy the condition $S(x)\leqq 1$; and that is, the condition

$$r_1+r_2+\cdots+r_s+2r_{s+1}+\cdots+2r_\nu\leqq 1.$$

To visualize the work, let $n=3$. If then all three functions of y are real, so that $\nu=3$, the surface $S(x)=1$ is the surface of the octahedron, the equations of whose eight faces are

$$\pm x\pm y\pm z=1.$$

If however, two of the functions y are conjugate imaginary, then $S(x)=1$ is the surface of a double cone which is generated by the revolution of a rhomb about its diagonal. Observe that the equations of the cones with vertices $\pm 1, 0, 0$, which stand on the circle $\frac{z^2+y^2}{r^2}=1$, in the zy-plane, are $\frac{z^2+y^2}{r^2}=(1\pm x)^2$. Hence, if $r=\frac{1}{2}$, we have the desired cones (Salmon, *Geometry of Three Dimensions*, p. 101, Ex. 7).

Noting [1] that when the integration is taken as indicated above, we have

$$J=\frac{2^{2\nu-n}\pi^{n-\nu}}{\Pi(n)\Delta},$$

where $\Pi(n)=1, 2, \cdots, n$.

From formula (vii) of Art. 146 it follows that

$$M^n\leqq\left(\frac{4}{\pi}\right)^{n-\nu}\Pi(n)\Delta, \qquad \text{(i)}$$

[1] See Dirichlet, *Werke*, Vol. I, p. 391; Kronecker, *Vorlesungen über einfach und mehrfach Integrale*, p. 243, Formula 10; Goursat, *Cours d'analyse*, Vol. I, p. 372; Humbert, *Cours d'analyse*, Vol. II, p. 102, derives a similar formula for the tetrahedron. See also Wilson's *Advanced Integral Calculus*.

where M is the least positive value which the function

$$|y_1|+|y_2|+\cdots+|y_n|$$

can take for integral values of $x_1, x_2, \cdots, x_n$.

The above limit may be put into a more simple form, if we observe that by definition of $\Pi(n)$

$$\frac{\Pi(n+1)}{(n+1)^{n+1}}=\frac{\Pi(n)}{(n+1)^n}=\frac{\Pi(n)}{n^n}\left(\frac{n}{n+1}\right)^n.$$

By the Binomial Theorem

$$\left(\frac{n+1}{n}\right)^n=\left(1+\frac{1}{n}\right)^n\geqq 2,$$

where the equality sign appears only when $n=1$.

It follows that

$$\frac{\Pi(n+1)}{(n+1)^{n+1}}\leqq\frac{1}{2}\,\frac{\Pi(n)}{n^n};$$

and by a repetition of this formula it is seen that

$$\Pi(n)\leqq\frac{n^n}{2^{n-1}}.$$

In this expression the equality sign appears only when $n=1$ and $n=2$. Observe also that ν is at least equal to 1, so that

$$2^{n-\nu}\leqq 2^{n-1}.$$

The formula for M above is thus transformed into

$$M\leqq\left(\frac{2}{\pi}\right)^{\frac{n-\nu}{n}} n\sqrt[n]{\Delta}.$$

In this formula the equality sign appears only when $n=1$ or $n=2$ and in the latter case only under the assumption that $\nu=1$; and that is, when y_1 and y_2 are conjugate imaginaries.

Since $\frac{2}{\pi}$ is less than unity, it is evident finally that

$$M\leqq n\sqrt[n]{\Delta},$$

where the equality sign appears, if $n=1$. Neglecting this case, the following theorem has been derived:

THEOREM. *If $y_1, y_2, \cdots, y_n$ is a system of linear functions which are real or are conjugate imaginary in pairs, with a determinant which does not vanish and is in absolute value $=\Delta$, then to the variables there may be ascribed integral values that do not all vanish such that the arithmetical mean of the absolute values of the y's is less than $\sqrt[n]{\Delta}$.*

ART. **149. Application to Algebraic Realms.** LEMMA. *If $a_1, a_2, \cdots, a_n$ are real positive quantities, then is*

$$a_1+a_2+\cdots+a_n \geqq n\sqrt[n]{a_1a_2\cdots a_n}.$$

The Lemma is evidently true for $n=2$, since

$$a_1+a_2-2\sqrt{a_1a_2}=(\sqrt{a_1}-\sqrt{a_2})^2$$

a quantity which is never negative. Hence, to make an inductive proof, suppose that the theorem is proved for $n-1$. If then a_n is a quantity which is as great as any of the preceding a's, it follows that

$$a_n \geqq \sqrt[n-1]{a_1\cdot a_2\cdots a_{n-1}}.$$

Denoting the expression on the right by b, we have by hypothesis

$$a_1+a_2+\cdots+a_{n-1} \geqq (n-1)b;$$

and consequently

$$a_1+a_2+\cdots+a_n \geqq a_n+(n-1)b.$$

From this it follows that

$$\frac{a_1+a_2+\cdots+a_n}{n} \geqq b+\frac{a_n-b}{n}.$$

By virtue of the Binomial Theorem, since a_n-b is not negative, we have

$$\left(\frac{a_1+a_2+\cdots+a_n}{n}\right)^n \geqq b^n+b^{n-1}(a_n-b)=a_nb^{n-1};$$

and with this the lemma is proved.

If in the above expression for the a's there are written the absolute values of the y's of Art. 148, there arises:

THEOREM I. *If $y_1, y_2, \cdots, y_n$ are linear functions of the variables $x_1, x_2, \cdots, x_n$, and if the y's are either all real or in part conjugate imaginary in pairs, with determinant whose absolute value is Δ, then for the x's such integral values may be found that the y's do not all vanish and are such that*

$$|y_1 \cdot y_2 \cdots y_n| < \Delta. \tag{1}$$

The theorem is true but loses its significance if the sum of the y's vanishes. A better defined limit for this product is had from (i) of the preceding article, namely

$$(|y_1| + \cdots + |y_n|)^n \leqq M^n \leqq \left(\frac{4}{\pi}\right)^{n-\nu} \Pi(n)\Delta,$$

or

$$(y_1 \cdot y_2 \cdots y_n) \leqq \left(\frac{4}{\pi}\right)^{n-\nu} \frac{\Pi(n)}{n^n}\Delta. \tag{2}$$

Observe (see for example Humbert, *Cours D'Analyse*, Vol. II, p. 100; and for the Sterling approximation, Wilson's *Advanced Calculus*, p. 458, Ex. 13) that

$$\Pi(n) < \sqrt{2\pi n}e^{-n+\frac{1}{12n}}n^n.$$

It results that

$$|y_1 \cdot y_2 \cdots y_n| \leqq \left(\frac{4}{\pi}\right)^{n-\nu} \sqrt{2\pi n}e^{-n+\frac{1}{12n}}\Delta. \tag{3}$$

From this, certain noteworthy results may be derived in the theory of algebraic numbers:

Let Ω be an algebraic realm, and let $\mathfrak{a}$ be an ideal in this realm with basis $\alpha_1, \alpha_2, \cdots, \alpha_n$ such that all integers in Ω which are divisible by $\mathfrak{a}$ may be expressed in the form

$$\alpha = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n,$$

where the x's are rational integers.

Next consider the n integers that are conjugate to α. These are n linear functions of the x's which do not

vanish unless all the x's are equal to zero. These functions may be written for the y's in the formulas above. The square of Δ is then the discriminant of the system of the quantities $\alpha^{(1)}, \alpha^{(2)}, \cdots, \alpha^{(n)}$, these quantities being the conjugate values of α just written.

Further (see Art. 137),

$$\pm\Delta^2 = N(\mathfrak{a})^2 D$$

where D is the discriminant (basal invariant) of the realm Ω. From formula (1) above is derived the theorem:

THEOREM II. *If $\mathfrak{a}$ is an ideal of the realm Ω, there is always an integer α in Ω that is different from zero, which is divisible by $\mathfrak{a}$ and is such that*

$$N(\alpha) < N(\mathfrak{a})\,|\sqrt{D}\,|.$$

(See Art. 137.) Since α is divisible by the ideal $\mathfrak{a}$, we may put $\frac{\alpha}{\mathfrak{a}} = \mathfrak{b}$, where $\mathfrak{b}$ is an integral ideal, or

$$\alpha = \mathfrak{a}\mathfrak{b}.$$

It follows from the theorem just proved that

$$N(\mathfrak{b}) < |\sqrt{D}\,|. \tag{4}$$

If $\bar{\alpha}$ is another integer in Ω that is divisible by $\mathfrak{a}$, so that

$$\bar{\alpha} = \mathfrak{a}\mathfrak{b}_1,$$

say, then is

$$\frac{\alpha}{\bar{\alpha}} = \frac{\mathfrak{b}}{\mathfrak{b}_1}, \qquad \text{or} \qquad \mathfrak{b} \sim \mathfrak{b}_1.$$

If then α passes over the collectivity of integers in Ω that are divisible by $\mathfrak{a}$, it is seen that $\mathfrak{b}$ goes through an ideal-class; and this, with what has just been proved gives expression to the theorem (see also Vol. I, Arts. 218 and 309):

THEOREM III. *In every ideal-class there is an ideal whose norm is less than $|\sqrt{D}\,|$.*

In formula (4) the equality sign can appear only when $n=1$. Further, since $N(\mathfrak{b})>1$, we have in (4) a proof of the theorem:

THEOREM IV. *Besides the realm*[1] *of rational integers there is no realm whose fundamental invariant* $D=\pm 1$. (See also Vol. I, Art. 298; and Minkowski, *Geometrie d. Zahlen*, p. 130.)

More definite limits may be derived for the absolute value of the discriminant of a realm, if formulas (2) and (3) above are used. From (3) it is seen that

$$|N(\alpha)|^2<\left(\frac{4}{\pi}\right)^{2(n-\nu)}\frac{(n!)^2}{n^{2n}}N(\mathfrak{a})^2|D|;$$

and since

$$\left|\frac{N(\alpha)}{N(\mathfrak{a})}\right|^2>1,$$

it follows that

$$|D|\geqq\left(\frac{\pi}{4}\right)^{2(n-\nu)}\frac{n^{2n}}{(n!)^2}. \tag{5}$$

Further from (3) it follows at once (see also Minkowski's *Geometrie der Zahlen*, p. 134) that

$$|D|>\left(\frac{\pi}{4}\right)^{2(n-\nu)}\frac{e^{2n-\frac{1}{6n}}}{2\pi n}. \tag{6}$$

Since the right-hand side of this expression becomes infinite with n, the theorem follows, namely:

THEOREM V. *A definite discriminant D is to be had only with a finite number of the integers n, which determine the degree of the realms.*

From (5) and in definite cases, other limits may be had for the discriminants. For example, if $n=2$ and $\nu=2$ there is a real quadratic realm, D is positive and at least is equal to 4. For an imaginary quadratic realm $n=2$,

[1] Kronecker, *Werke*, Vol. II, p. 269; Minkowski, *Werke*, Vol. I, pp. 259 and 262.

$\nu = 1$, D is negative and in absolute value is greater than $\frac{\pi^2}{4}$; and that is, $D \leqq -3$ (see Vol. I, Art. 93).

For $n = 3$, and that is, for cubic realms, it is seen that D is greater than 20 or less than -12.

Further, see Minkowski, *Geometrie der Zahlen*, §§ 30, 34, 35, 37, 40; and also Hermite, *Crelle's Journal*, Vol. 40, p. 263; Vol. 47, p. 335; Vol. 53, p. 182. This work of Hermite's was the inspiration of much of Minkowski's endeavors. See p. 122 of Minkowski's work just mentioned.

CHAPTER IX

THE NUMBER OF IDEAL-CLASSES IN A FIXED REALM

ART. 150. **Synopsis of Parts of the Theory That Have Been Proved in the Preceding Chapters.** Let Ω be a realm of the nth degree and let $\Omega(=\Omega_1), \Omega_2, \cdots, \Omega_n$ be the conjugate realms. The irreducible equation whose roots determine these realms will in general have real and imaginary roots. The imaginary roots appear in pairs, so that to every imaginary realm Ω_s there is associated another imaginary realm $\Omega_{s'}$, in which the numbers are the conjugate imaginaries of the numbers in $\Omega_{s'}$, so that $\Omega_{s'}$ is derived from Ω_s through the substitution $(i, -i)$.

The number of pairs of imaginary roots plus the number of real roots was denoted (Art. 112) by ν. If all the roots are real, then is $n=\nu$; if they are all imaginary, then is $n=2\nu$. The number of pairs of imaginary realms is $n-\nu$, and the number of real realms is $2\nu-n$ (Art. 112).

If $\omega_1, \omega_2, \cdots, \omega_n$ is a basis of all integers of Ω (Vol. I, Art. 93), and if

$$\omega_1^{(s)}, \omega_2^{(s)}, \cdots, \omega_n^{(s)} \qquad (s=1, 2, \cdots, n)$$

denote the conjugate systems, then all integers of the realms Ω_s may be expressed in the form

$$\eta^{(s)}=x_1\omega_1^{(s)}+x_2\omega_2^{(s)}+\cdots+x_n\omega_n^{(s)} \quad (s=1, 2, \cdots, n), \tag{1}$$

where the x's are rational integers; and the fundamental invariant of the realm Ω is the square of the determinant

$$\sqrt{D}=\sum\pm\omega_1^{(1)}\omega_2^{(2)}\cdots\omega_n^{(n)}.$$

Through the substitution $(i, -i)$ any two imaginary rows of this determinant are interchanged, so that $\sqrt{D}$ changes its sign only if the number of pairs of conjugate roots is odd and if $n-\nu$ is odd. In this case $\sqrt{D}$ is imaginary; otherwise, $\sqrt{D}$ is real. It follows that the discriminant of the realm Ω is positive or negative according as $n-\nu$ is even or odd.

The system (1) is a system of linear equations in the x's, whose determinant is different from zero. If we assume that the absolute values of $\eta^{(s)}$ do not exceed certain fixed limits, we have, by solving these equations, definite limits for the rational integers x. This gives expression to the theorem (see Art. 125):

THEOREM. *There exists in any algebraic realm Ω only a finite number of algebraic integers such that the absolute values of the conjugate integers $\eta^{(s)}$ all lie within given fixed limits.*

Now let $r_1, r_2, \cdots, r_n$ be a system of real (not necessarily rational quantities), such that

$$r_1 \cdot r_2 \cdots r_n = 1, \tag{2}$$

with the further condition that if $\eta^{(s)}$ and $\eta^{(s')}$ are two conjugate integers, then

$$r_s = r_{s'}; \tag{3}$$

and for the y's of the *theorem* at the end of Art. 148 write

$$\frac{\eta^{(1)}}{r_1}, \frac{\eta^{(2)}}{r_2}, \cdots, \frac{\eta^{(n)}}{r_n}.$$

It results that

$$\left|\frac{\eta^{(1)}}{r_1}\right| + \left|\frac{\eta^{(2)}}{r_2}\right| + \cdots + \left|\frac{\eta^{(n)}}{r_n}\right| < n\left|\sqrt[2n]{D}\right|.$$

Denote the right-hand side of this expression by A and observe that none of the quantities that constitute the sum on the left-hand side can reach the value A.

This result may be expressed as follows:

THEOREM. *If r_s is an arbitrary system of real positive quantities subject to the two conditions (2) and (3), there is a real quantity A determined through the realm Ω, such that an algebraic integer η of the realm Ω may be determined which with its conjugate integers satisfy the inequalities*

$$|\eta^{(s)}| < r_s A \qquad (s=1, 2, \cdots, n). \tag{4}$$

Observe that except in the realm of rational numbers where $n=1$ and in the imaginary quadratic realms ($n=2$, $\nu=1$) one of the numbers r_s is perfectly arbitrary. Accordingly, there results from (4) the theorem:

THEOREM. *In every algebraic realm, the rational and quadratic imaginary realms excepted, there exists an algebraic integer which is in absolute value less than any fixed limit, however small.*

If of two conjugate complex realms only one is taken, there remains the series of conjugate realms $\Omega_1, \Omega_2, \cdots, \Omega_\nu$. With this system of realms we may associate a system of symbols $c_1, c_2, \cdots, c_\nu$, which are such that each of the c's that are associated with real realms has the value 1, while the other c's have the value 2. It follows that

$$\sum_{s=1}^{s=\nu} c_s = n.$$

Now let η be any number ($\neq 0$) of the realm, and let $\eta^{(1)}, \eta^{(2)}, \cdots, \eta^{(n)}$ be the conjugate quantities. Corresponding to this system of η's arrange another system of quantities $L_1, L_2, \cdots, L_n$ defined through the equations

$$L_s = c_s \log |\eta^{(s)}|.$$

If Ω_s is real and the sign $\pm$ is chosen so that $\pm\eta_s$ is positive, then is $L_s = \log(\pm\eta^{(s)})$. If, however, $\eta^{(s)}, \eta^{(s')}$ are a pair of complex quantities, then is

$$L_s = \log \eta^{(s)} \cdot \eta^{(s')}.$$

Observe that to $\eta^{(s)}$ and $\eta^{(s')}$ there belongs the same L_s, so that the number of different L_s is equal to ν.

ART. **151. Reduced Numbers.** Let α be any number of the realm Ω and denote the system of conjugate logarithms of α by

$$L_1=c_1 \log |\alpha^{(1)}|,\ L_2=c_2 \log |\alpha^{(2)}|,\ \cdots,\ L_\nu=c_\nu \log |\alpha^{(\nu)}|,$$

where $c_1+c_2+\cdots+c_\nu=n$. Let $\epsilon_1,\ \epsilon_2,\ \cdots,\ \epsilon_{\nu-1}$ be a system of fundamental units with comjugate logarithms

$$\epsilon_k: \qquad l_k^{(1)},\ l_k^{(2)},\ \cdots,\ l_k^{(\nu)} \qquad (k=1, 2, \cdots, \nu-1).$$

Then as in Art. 140, it is possible to determine real quantities x such that the following linear equations are satisfied:

$$(1) \qquad \begin{cases} x_1 l_1^{(1)}+x_2 l_2^{(1)}+\cdots+x_{\nu-1} l_{\nu-1}^{(1)}+x_\nu c_1=L_1, \\ x_1 l_1^{(2)}+x_2 l_2^{(2)}+\cdots+x_{\nu-1} l_{\nu-1}^{(2)}+x_\nu c_2=L_2, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ x_1 l_1^{(\nu)}+x_2 l_2^{(\nu)}+\cdots+x_{\nu-1} l_{\nu-1}^{(\nu)}+x_\nu c_\nu=L_\nu. \end{cases}$$

Observe (see Art. 138) that

$$l_s^{(1)}+l_s^{(2)}+\cdots+l_s^{(\nu)}=\log|N(\epsilon_s)|=0 \quad (s=1, 2, \cdots, \nu-1).$$

It follows that (Art. 122, end)

$$\begin{vmatrix} l_1^{(1)}, & l_2^{(1)}, & \cdots, & l_{\nu-1}^{(1)}, & c_1 \\ l_1^{(2)}, & l_2^{(2)}, & \cdots, & l_{\nu-1}^{(2)}, & c_2 \\ \cdots\cdots & \cdots\cdots & \cdots & \cdots\cdots & \cdots\cdots \\ l_1^{(\nu)}, & l_2^{(\nu)}, & \cdots, & l_{\nu-1}^{(\nu)}, & c_\nu \end{vmatrix} = nL(\epsilon_1, \epsilon_2, \cdots, \epsilon_{\nu-1}),$$

which determinant is $\neq 0$. The unknown quantities x_1, $x_2,\ \cdots,\ x_{\nu-1}$ are therefore uniquely determined, and these quantities are called the *exponents* of the number α with respect to the fundamental system of units $\epsilon_1, \epsilon_2, \cdots, \epsilon_{\nu-1}$. Since (Art. 150) $c_1+c_2+\cdots+c_\nu=n$, it is seen that through the addition of the equations (1)

$$nx_\nu=\log|N(\alpha)|=\log|N(\eta\alpha)|,$$

where η is an arbitrary unit of Ω.

It is evident that the exponents of a product or quotient is equal to the sum or the difference of the corresponding exponents of the product or quotient. The exponents of a unit are rational integers (Art. 111), and every system of rational integers $x_1, x_2, \cdots, x_{\nu-1}$ constitute an exponent-system of a unit.

The exponent-systems of associated (Vol. I, Art. 91) numbers differ from one another by integral values, so that corresponding to every number α we can find an associated number α_0 whose exponents lie between 0 and 1. Such numbers are called *reduced numbers* with regard to the fundamental system of units $\epsilon_1, \epsilon_2. \cdots, \epsilon_{\nu-1}$.

It was seen in Art. 141 that all reduced units and only such units satisfy an equation $x^w = 1$; and that is, they are roots of unity, in number w.

We thus have the theorem:

THEOREM. *Corresponding to every number α of Ω there are w and no more reduced numbers $\rho\alpha_0$, where ρ is a root of $x^w = 1$.*

ART. **152. Limits Restricting the Number of Algebraic Integers of Ω Which Are Divisible by an Ideal.** It was proved in Art. 25 that every integer in Ω was divisible by only a finite number of ideals. Since every integral ideal is a divisor of its norm, there are only a finite number of integral ideals in Ω, whose absolute norms lie within a fixed limit.

The question [1] before us is *to determine the number T of all principal ideals (and that is, of all algebraic integers) of the realm Ω whose absolute norms are less than a positive quantity t and which are divisible by a given ideal $\mathfrak{a}$.*

The analogous question in the realm of rational integers is *to determine the number T of rational integers, which are*

[1] The methods followed here are essentially those found in Dirichlet-Dedekind, *Zahlentheorie*, pp. 603 ff. See also Weber, *Algebra*, Vol. II, pp. 710–727.

less than t and which are divisible by a rational integer m.

It is evident that T is the greatest integer in $\frac{t}{m}$, which integer is written $\left[\frac{t}{m}\right]$. Since

$$T=\frac{t}{m}+\frac{r}{m}, \qquad \text{where} \qquad r<m,$$

it is seen that

$$\frac{T}{t}=\frac{1}{m}+\frac{r}{tm}, \qquad \text{so that} \qquad \lim_{t\to\infty}\frac{T}{t}=\frac{1}{m}.$$

Let $\alpha_1, \alpha_2, \cdots, \alpha_n$ be a basis of $\mathfrak{a}$ and let $y=\alpha$ be any integer that is divisible by $\mathfrak{a}$, so that

$$y=\alpha=\alpha_1x_1+\alpha_2x_2+\cdots+\alpha_nx_n;$$

and put

$$\begin{aligned}
y_1&=\alpha_1^{(1)}x_1+\alpha_2^{(1)}x_2+\cdots+\alpha_n^{(1)}x_n,\\
y_2&=\alpha_1^{(2)}x_1+\alpha_2^{(2)}x_2+\cdots+\alpha_n^{(2)}x_n,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
y_n&=\alpha_1^{(n)}x_1+\alpha_2^{(n)}x_2+\cdots+\alpha_n^{(n)}x_n,
\end{aligned} \tag{1}$$

where the x's are rational integers.

Denote the determinant of the system of equations (1) by A, so that

$$A=\sum\pm\alpha_1^{(1)}\alpha_2^{(2)}\cdots\alpha_n^{(n)}.$$

It is proved in Art. 137 that

$$A^2=N(\mathfrak{a})^2\cdot D,$$

where D is the discriminant of Ω. As in Art. 144 let x_1, $x_2, \cdots, x_n$ be the coördinates of a point x in an n-dimensional space, and corresponding to each lattice-point x, let there be a point x' whose coördinates are determined through the equations

$$x_1'=t^nx_1,\ x_2'=t^nx_2,\ \cdots,\ x_n'=t^nx_n,$$

t being the positive quantity indicated above.

To each domain S of points x, there corresponds a domain S' of points x'. All figures in S are similar to the

corresponding figures in S' and the linear dimensions in S are to those in S' as $1 : t^{\frac{1}{n}}$. If then the domain S is given, the corresponding domain S' is dependent upon t, becoming larger the larger t is taken.

The number of lattice-points which lie within a finite domain S' is finite but increases with t and is denoted here by N_t. Construct around each of these lattice-points a cell whose edge has a length 1. To each of these cells there corresponds another cell whose center lies in S and whose edge has a length $\frac{1}{t^{\frac{1}{n}}}$, the volume of the cell being $\frac{1}{t}$.

Due to Art. 145, the volume of the domain S, and that is, of the integral

$$V = \int\int \cdots \int dx_1 \cdot dx_2 \cdots dx_n$$

is equal to the limiting value (t becoming infinite) of the ratio

$$V = \operatorname*{Lim}_{t \to \infty} \frac{N_t}{t}.$$

See Art. 144, end, where here $\frac{1}{t^{\frac{1}{n}}} = \delta$. Observe that through the linear equations (1) every lattice point x is the *image* or *picture* of an algebraic integer y of the realm Ω, so that N_t is also the *number of integers* in Ω which are divisible by $\mathfrak{a}$, and whose images lie in S'.

We shall next limit the domain S in such a way that of the infinite assemblage of associated numbers to which the same principal ideal (algebraic integer) corresponds, there is only a fixed definite number which have their images in S'. With this in view choose a system of fundamental units in Ω, say $\epsilon_1, \epsilon_2, \cdots, \epsilon_{\nu-1}$, whose conjugate logarithms are (Art. 121)

$$l_i^{(1)}, l_i^{(2)}, \cdots, l_i^{(\nu)} \qquad (i = 1, 2, \cdots, \nu - 1).$$

The quantities y_i being defined through the equations (1), let

$$z_i = c_i \log |y_i|$$

so that, when x_i denote a system of rational integers, z_i denotes the system of conjugate logarithms of the algebraic integer $\alpha = y$. If then (Art. 121) y_k belongs to a real realm, then is

$$z_k = \tfrac{1}{2} \log y_k^2;$$

and, when y_k, y_k' belong to a pair of complex imaginary values, then is

$$z_k = \tfrac{1}{2} \log y_k \cdot y_k'.$$

Next determine the quantities $\xi_1, \xi_2, \cdots, \xi_{\nu-1}, \xi_\nu$ through the linear equations

$$\begin{aligned}
&\xi_1 l_1^{(1)} + \xi_2 l_2^{(1)} + \cdots + \xi_{\nu-1} l_{\nu-1}^{(1)} + c_1 \xi_\nu = z_1, \\
&\xi_1 l_1^{(2)} + \xi_2 l_2^{(2)} + \cdots + \xi_{\nu-1} l_{\nu-1}^{(2)} + c_2 \xi_\nu = z_2, \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
&\xi_1 l_1^{(\nu)} + \xi_2 l_2^{(\nu)} + \cdots + \xi_{\nu-1} l_{\nu-1}^{(\nu)} + c_\nu \xi_\nu = z_\nu,
\end{aligned}$$

whose determinant (Art. 122) $\neq 0$. Through the addition of these equations it is evident (Art. 138) that

$$\xi_\nu = \frac{1}{n} \log |N(\alpha)| = \frac{1}{n} \log |N(y)|. \tag{2}$$

Observe that through the substitutions $x_i' = t^{\frac{1}{n}} x_i$, we have the relations $y_i' = t^{\frac{1}{n}} y_i$ and

$$z_i' = c_i \log y_i' = c_i \log \left(t^{\frac{1}{n}} y_i \right),$$

or,

$$z_i' = z_i + \frac{1}{n} c_i \log t.$$

It follows also that

$$\xi_1' l_1^{(i)} + \xi_2' l_2^{(i)} + \cdots + \xi_{\nu-1}' l_{\nu-1}^{(i)} + c_i \xi_\nu' = z_i' = z_i + \frac{1}{n} c_i \log t,$$

or,

$$\xi_1' = \xi_1, \ \xi_2' = \xi_2, \ \cdots, \ \xi_{\nu-1}' = \xi_{\nu-1}, \ \xi_\nu' = \xi_\nu + \frac{1}{n} \log t. \tag{3}$$

Finally limit the domain S' by restricting $\xi_1', \xi_2', \cdots, \xi_\nu'$ so that

$$(4) \qquad 0 \leqq \xi_1' < 1, \cdots, 0 \leqq \xi_{\nu-1}' < 1, \ \xi_\nu' < \frac{1}{n}\log t;$$

$$\text{and as} \quad \xi_\nu' = \xi_\nu + \frac{1}{n}\log t, \quad \text{we have} \quad \xi_\nu < 0.$$

We are thus able to bring it about that the lattice-points x' in S' represent only reduced integers γ, say; and due to (2) all and only such lattice-points whose norms in absolute value are less than t are so represented.

Among the reduced integers, as shown at the end of the preceding article, there are always w associated with one another, where w is the number of the roots of unity in Ω. If the number of such associated integers are gathered into one complex, the number of such complexes is equal to the number T of all not associated integers in Ω, which are divisible by $\mathfrak{a}$ and whose absolute norms are less than t.

Accordingly, the number of the lattice-points situated in the domain S' is

$$N_t = wT.$$

For the boundaries of the domain S we have from (3) and (4)

$$0 \leqq \xi_1 < 1, \cdots, 0 \leqq \xi_{\nu-1} < 1, \ \xi_\nu < 0.$$

From above,

$$\lim_{t\to 0} \frac{T}{t} = \frac{1}{w} \lim_{t\to\infty} \frac{N_t}{t} = \frac{1}{w} \int\int \cdots \int dx_1 \cdot dx_2 \cdots dx_n,$$

the limits to be taken as just indicated.

ART. 153. **Computation of the Volume V.** The limits above for the determination of the volume of S depend only upon the absolute value of the variables y_i, so that

the formula of Art. 148 may be used. That formula was

$$V=\frac{2^n\pi^{n-\nu}}{\Delta}\int\int\cdots\int r_{s+1}r_{s+2}\cdots r_\nu dr_1dr_2\cdots dr_\nu,$$

where the r's are the absolute values of the y's.

Hence, since

$$z_i=c_i\log r_i,$$

it is seen that

$$c_idr_i=e^{\frac{z_i}{c_i}}dz_i \qquad \text{and} \qquad c_ir_idr_i=e^{\frac{2z_i}{c_i}}dz_i.$$

The number of pairs of imaginary (conjugate complex) y's is $n-\nu$, while the real y's are $s=2\nu-n$ in number.

Further, $c_i=1$ for $i=1, 2, \cdots, s$ and $c_i=2$ for $i=s+1, s+2, \cdots, \nu$. Hence, the formula above may be written

$$V=\frac{2^\nu\pi^{n-\nu}}{\Delta}\int\int\cdots\int e^{z_1+z_2+\cdots+z_\nu}dz_1dz_2\cdots dz_\nu.$$

Next introduce the variables ξ's of the preceding article, and observe that

$$\frac{d(z_1,\ z_2,\ \cdots,\ z_\nu)}{d(x_1,\ x_2,\ \cdots,\ x_\nu)}=\begin{vmatrix} l_1^{(1)}, & l_2^{(1)}, & \cdots, & l_{\nu-1}^{(1)}, & c_1 \\ l_1^{(2)}, & l_2^{(2)}, & \cdots, & l_{\nu-1}^{(2)}, & c_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ l_1^{(\nu)}, & l_2^{(\nu)}, & \cdots, & l_{\nu-1}^{(\nu)}, & c_\nu \end{vmatrix},$$

which determinant (Art. 151) $=nL(\epsilon_1, \cdots, \epsilon_{\nu-1})$. If we note that (Art. 152)

$$z_1+z_2+\cdots+z_n=n\xi_\nu$$

and for brevity put $L(\epsilon_1, \epsilon_2, \cdots, \epsilon_{\nu-1})=L$, it is seen that

$$V=\frac{2^\nu\pi^{n-\nu}}{\Delta}nL\int_{-\infty}^{0}e^{n\xi_\nu}d\xi_\nu\int_0^1 d\xi_1\int_0^1 d\xi_2\cdots\int_0^1 d\xi_{\nu-1}=\frac{2^\nu\pi^{n-\nu}L}{\Delta}.$$

In this formula Δ is the absolute value of the determinant of the linear equations (1), which determine the y's of Art. 152. This determinant was denoted above by A; and in that article it was seen that

$$A^2=N(\mathfrak{a})^2|D|.$$

The formula at the end of the last article may therefore be

written

$$\lim_{t\to\infty}\frac{T}{t}=\frac{2^{\nu}\pi^{n-\nu}L}{wN(\mathfrak{a})\,|\sqrt{D}\,|}.$$

If we put

(1)
$$g=\frac{2^{\nu}\pi^{n-\nu}L}{w\,|\sqrt{D}\,|},$$

it is seen that

$$\lim_{t\to\infty}\frac{T}{t}=\frac{g}{N(\mathfrak{a})},$$

where g is a definite positive number that is determined completely through the nature of the realm Ω.

Remark. It may happen (see Dirichlet-Dedekind, p. 578) that the norms of all the integers, say $\epsilon\mu$, that are associated with μ, are *negative*, a case which always happens and only happens if in the realm Ω there exist integers with negative norm, but in which there are no units with negative norm. The degree of such a realm must be even and among the conjugate realms there must be such which consist of only real numbers; for example, the quadratic realm in which $D=+12$. In this case it is sometimes advantageous to call two ideals $\mathfrak{a}$ and $\mathfrak{a}'$ equivalent, only if there exists a number η with *positive* norm which satisfies the condition $\mathfrak{a}\eta=\mathfrak{a}'$. Accordingly the number of classes is doubled. The principal class H consists then only of those principal ideals $\mathfrak{o}\mu$, which correspond to the integers μ with positive norm, while the remaining principal ideals form a separate class.

The formula above thus modified becomes

$$\lim_{t\to\infty}\left(\frac{T}{t}\right)=\frac{2^{\nu-\sigma}\pi^{n-\nu}Q}{N(\mathfrak{a})\sqrt{\pm D}},$$

where $Q=\dfrac{L}{w}$, and where $\sigma=0$ or 1, according as the realms conjugate to Ω are all imaginary or not. In the latter case the condition that the norm of μ must be *positive* diminishes the number g by one half.

Further, observe that in the above limit the factor $\frac{2^{\nu}\pi^{n-\nu}}{N(\mathfrak{a})\sqrt{\pm D}}$ depends upon the nature of the realm, while Q does not, so that the ratio $\frac{|l_k(\epsilon_i)|}{w}$ is constant for any system of independent units $\epsilon_1, \epsilon_2, \cdots, \epsilon_{\nu-1}$ as well as for the fundamental system of such units.

ART. **154. A Digression into the Dirichlet Series.**[1]

THEOREM I. *If* $a_1, a_2, \cdots, a_n, \cdots$, *is an unlimited system of positive, negative or vanishing quantities, and if it is assumed that the sum*

$$\sigma_n = a_1 + a_2 + \cdots + a_n \tag{1}$$

for every arbitrary value of n remains in absolute value less than a finite limit C, then is the series

$$S = \frac{a_1}{1^s} + \frac{a_2}{2^s} + \frac{a_3}{3^s} + \cdots \tag{2}$$

not only convergent for every positive value of s, but the series also expresses a continuous function of s.

To prove this theorem, distribute the terms in S in such a way that

$$S = S_m + R_m,$$

where

$$S_m = \frac{a_1}{1^s} + \frac{a_2}{2^s} + \cdots + \frac{a_{m-1}}{(m-1)^s},$$

$$R_m = \frac{a_m}{m^s} + \frac{a_{m+1}}{(m+1)^s} + \frac{a_{m+2}}{(m+2)^s} + \cdots.$$

Due to (1) it is seen that

$$a_m = \sigma_m - \sigma_{m-1}, \quad a_{m+1} = \sigma_{m+1} - \sigma_m, \quad a_{m+2} = \sigma_{m+2} - \sigma_{m+1}, \quad \cdots,$$

[1] See for example, Bachmann, *Die analytische Zahlentheorie*, Chap. III; and Landau, *Handbuch der Lehre von der Vertheilung der Primzahlen*. See also Weber, *Algebra*, Vol. II, §§ 196–198.

and consequently

$$R_m+\frac{\sigma_{m-1}}{m^s}=\sigma_m\left(\frac{1}{m^s}-\frac{1}{(m+1)^s}\right)$$
$$+\sigma_{m+1}\left(\frac{1}{(m+1)^s}-\frac{1}{(m+2)^s}\right)+\cdots.$$

By hypothesis σ_{m-1}, σ_m, σ_{m+1}, $\cdots$, are included between finite limits $\pm C$. It follows that $R_m+\frac{\sigma_{m-1}}{m^s}$ lies between the two limits

$$\pm C\left(\frac{1}{m^s}-\frac{1}{(m+1)^s}+\frac{1}{(m+1)^s}-\frac{1}{(m+2)^s}+\cdots\right)=\pm\frac{C}{m^s},$$

with the result that in absolute value

$$R_m<\frac{2C}{m^s};$$

or, if $s>c$,

$$R_m<\frac{2C}{m^c}.$$

This upper limit of R_m which is independent of s, may, if c is positive, be suppressed under any limit however small, by taking m sufficiently large.

From this it is seen that S is not only convergent but also it is a continuous function of s. For, by taking m sufficiently large, not only is R_m but also the oscillation of R_m with variable s, is indefinitely small.

Observe that the hypothesis regarding σ_m no wise presupposes the convergence of the infinite series (1). It is not necessary that the quantities a_k be real; for, were they imaginary, it would only be necessary to apply the theorem to the real and the imaginary component S. It is not necessary to assume that the quantities a_1, a_2, a_3, $\cdots$ are constants. The theorem remains true if these quantities are continuous functions of s.

THEOREM II. *Let $\mu_1, \mu_2, \mu_3, \cdots$ be an infinite assemblage of positive quantities, such that only a finite number $Z(t)$ of them is not greater than a finite quantity t; and suppose that a finite positive* quantity *C may be determined, that is independent of t, and is such that*

$$Z(t) < Ct; \tag{1}$$

and further, let $F(t)$ be a function that is positive for positive values of t and which decreases in value with increasing values of t and is such that the infinite series

$$R = F(1) + F(2) + F(3) + \cdots = \sum_{h=1}^{h=\infty} F(h) \tag{2}$$

is convergent. Then the infinite series

$$S_t = \sum F(\mu), \qquad (\mu \leqq t) \tag{3}$$

has a definite limit S when t becomes indefinitely large.

The infinite series (2) is taken over all positive rational integers h, while S is to be so chosen that the summation is over all the quantities μ that are not greater than t, and finally t is allowed to become indefinitely large.

The number of μ's which are situated between two consecutive integers h and $h+1$, the upper limit included, is $Z(h+1) - Z(h)$; and since by hypothesis the function $F(t)$ decreases with increasing t, it follows that

$$\sum_{h<\mu\leq h+1} F(\mu) < [Z(h+1) - Z(h)]F(h), \tag{4}$$

an inequality which still exists if by $F(0)$ is understood a quantity, which is greater than any of the quantities $F(\mu)$.

If n is any integer which satisfies the inequality

$$n < t \leqq n+1,$$

it follows from (3) and (4) that

$$S_t < \sum_{h=0}^{h=n} [Z(h+1) - Z(h)]F(h);$$

and this may be written, since $Z(0)=0$,

$$S_t<\sum_{h=1}^{h=n} Z(h)[F(h-1)-F(h)]+Z(n+1)F(n).$$

Since the difference $F(h-1)-F(h)$ is positive as is also the function $F(n)$, it follows from (1) that

$$S_t<C\{\sum_{h=1}^{h=n} h[F(h-1)-F(h)]+(n+1)F(n)\};$$

and that is,

$$S_t<C\sum_{h=0}^{h=n} F(h),$$

which proves Theorem II.

Next let the system of quantities $\mu_1, \mu_2, \mu_3, \cdots$, be arranged in such a way that

$$\mu_1 \leqq \mu_2 \leqq \mu_3 \leqq \cdots, \tag{i}$$

and as above, let $Z(t)$ denote the number of the quantities μ which are not greater than t. The following theorem may then be proved. (Weber, *Algebra*, Vol. II, p. 719.)

THEOREM III. *If one of the two limits*

$$\operatorname{Lim}_{n\to\infty} \frac{n}{\mu_n}, \qquad \operatorname{Lim}_{t\to\infty} \frac{Z(t)}{t}$$

is finite, the other also has a finite value.

First suppose that

(1) $$\operatorname{Lim}_{n=\infty} \frac{n}{\mu_n}=\gamma,$$

where γ is a definite quantity. In this case, when n becomes indefinitely large, the quantities μ_n must become indefinitely large. And for every positive t, there must be a value m, so that

(2) $$\mu_m \leqq t<\mu_{m+1}.$$

Observe that m becomes indefinitely large with t and due to (i),

$$Z(t)=m.$$

Hence, from (2)

$$\frac{m}{\mu_m} \leqq \frac{Z(t)}{t} > \frac{m}{\mu_{m+1}} = \frac{m+1}{\mu_{m+1}} \cdot \frac{m}{m+1};$$

and, as $\frac{m}{m+1}$ has 1 as limit when $m \to \infty$, it follows from (1) that

$$\text{(3)} \qquad \operatorname*{Lim}_{t=\infty} \frac{Z(t)}{t} = \gamma.$$

Secondly, suppose that (3) is true. In this case μ_n must become indefinitely large with n, otherwise, since the collectivity of all the μ's is infinite, $Z(t)$ would be infinite for a finite t and γ could not be finite.

Next suppose that μ_n is one of the μ's that appears among equal values, say,

$$\mu_{m+1}, \mu_{m+2}, \cdots, \mu_{m+l},$$

so that

$$m+1 \leqq n \leqq m+l.$$

It is evident that $Z(t)$ increases suddenly by l units as t passes through the value μ_n and that the ratio $\frac{Z(t)}{t}$ increases by $\frac{l}{\mu_n}$. Since, however, $\frac{Z(t)}{t}$ has a finite limit, it follows that

$$\operatorname*{L}_{n \to \infty} \frac{l}{\mu_n} = 0.$$

If $t = \mu_n$, then is $Z(t) = m+l$, and consequently,

$$\frac{Z(t)}{t} = \frac{m+l}{\mu_n} \qquad \text{and} \qquad \operatorname*{Lim}_{n=\infty} \frac{m+l}{\mu_n} = \gamma.$$

Further since

$$\text{(a)} \qquad \frac{m}{\mu_n} < \frac{n}{\mu_n} \leqq \frac{m+l}{\mu_n},$$

it is seen that

$$\operatorname{Lim}_{n\to\infty}\frac{n}{\mu_n}=\operatorname{Lim}_{n\to\infty}\frac{m}{\mu_n}=\gamma,$$

or, from (3) follows [1] (1).

THEOREM IV. *If the quantities* $\mu_1, \mu_2, \mu_3, \cdots$ *are such that*

$$\operatorname{Lim}_{t\to\infty}\frac{Z(t)}{t}=\gamma,$$

where γ *is a finite quantity, then is the series*

$$S=\frac{1}{\mu_1^s}+\frac{1}{\mu_2^s}+\frac{1}{\mu_3^s}+\cdots=\sum\frac{1}{\mu^s}\cdots \qquad \text{(i)}$$

convergent for every value of s *that is greater than 1 and further*

$$\operatorname{Lim}(s-1)S=\gamma. \qquad \text{(ii)}$$

If s is greater than 1, the series S is a special case of the series treated in Theorem II, since the series $1+\frac{1}{2^s}+\frac{1}{3^s}+\cdots$ is convergent if $s>1$. And with this follows the first part of Theorem IV.

To prove the second part of the theorem, choose two quantities α and β [see formula (a) under Theorem III above], such that

$$\alpha<\gamma<\beta,$$

and that as soon as $n\geqq m$, we have

$$\frac{\alpha}{n}<\frac{1}{\mu_n}<\frac{\beta}{n}. \qquad (1)$$

Due to Theorem III it is seen that α and β may be brought arbitrarily near together, if m is taken sufficiently large.

Next write

$$R_m=\sum_{n=\infty}^{n=m}\frac{1}{\mu_n},$$

[1] See Dirichlet-Dedekind, *Zahlentheorie*, Supplement II; Riemann, *Mathematische Werke*, Vol. II, No. 30; and also Dirichlet's *Werke*, Vol. I, pp. 357, 411.

and note from (1) that

$$\alpha^s \sum_{n=m}^{n=\infty} \frac{1}{n^s} < R_m < \beta^s \sum_{n=m}^{n=\infty} \frac{1}{n^s}. \tag{2}$$

Further, observe that

$$\int_n^{n+1} \frac{dx}{x^s} = \frac{1}{1-s}\left[\frac{1}{(n+1)^{s-1}} - \frac{1}{n^{s-1}}\right] = \frac{1}{1-s} \cdot \frac{1}{n^{s-1}} \times \left[\frac{1}{\left(1+\frac{1}{n}\right)^{s-1}} - 1\right]$$

$$= \frac{1}{1-s}\left[1 + \frac{1-s}{n} - k(1-s) - 1\right]\frac{1}{n^{s-1}} = \frac{1}{n^s} - k,$$

where k is a positive quantity.

It follows that

$$\int_n^{n+1} \frac{dx}{x^s} < \frac{1}{n^s} < \int_{n-1}^{n} \frac{dx}{x^s},$$

and consequently

$$\int_\infty^m \frac{dx}{x^s} < \sum_{n=\infty}^{n=m} \frac{1}{n^s} < \int_\infty^{m-1} \frac{dx}{x^s},$$

or,

$$\frac{1}{(s-1)m^{s-1}} < \sum_{n=\infty}^{n=m} \frac{1}{n^s} < \frac{1}{(s-1)(m-1)^{s-1}}.$$

Hence, from (2) it is seen that

$$\frac{\alpha^s}{m^{s-1}} < (s-1)R_m < \frac{\beta^s}{(m-1)^{s-1}}.$$

Writing

$$S = S_m + R_m,$$

we have

$$(s-1)S_m + \frac{\alpha^s}{m^{s-1}} < (s-1)S < (s-1)S_m + \frac{\beta^s}{(m-1)^{s-1}}.$$

In this expression keep m fixed and let s approach the value 1, and observe that $(s-1)S_m$ approaches the value zero. It follows that

$$\alpha = \lim_{s \to 1} (s-1)S < \beta, \tag{3}$$

an expression in which every trace of m has disappeared. Since both α and β differ from γ by arbitrarily small quantities, the truth of Theorem IV is evident.

It follows at once as an example that

$$\lim_{s\to 1}(s-1)\left[1+\frac{1}{2^s}+\frac{1}{3^s}+\cdots\right]=1.$$

THEOREM V. *If the quantities $\mu_1, \mu_2, \mu_3, \cdots$ have the property required in Theorem IV and if besides*

$$\gamma\mu_n - n = c_n, \tag{1}$$

where c_n is not infinite, when n becomes indefinitely large, and if further S has the meaning given to it in Theorem IV, then is

$$S-\frac{\gamma}{s-1}=C_s, \tag{2}$$

for $s>1$, a function of s which approaches a definite limit C_1 when $s-1$ becomes indefinitely small.

To prove this theorem, observe first that

$$S=\frac{1}{\mu_1^s}+\frac{1}{\mu_2^s}+\frac{1}{\mu_3^s}+\cdots.$$

Since

$$\sum^n\frac{\gamma^s}{n^s}-S=\gamma^s\left[\sum^n\frac{1}{n^s}-\frac{S}{\gamma^s}\right]=\gamma^s\left[\sum^n\frac{1}{n^s}-\frac{1}{\mu_1^s\gamma^s}-\frac{1}{\mu_2^s\gamma^s}\cdots\right],$$

it follows from (1) that

$$\sum^n\frac{\gamma^s}{n^s}-S=\gamma^s\sum^n\frac{1}{n^s}\left[1-\left(1+\frac{c_n}{n}\right)^{-s}\right]. \tag{3}$$

If ϵ denotes a positive proper fraction, and if we put

$$a_n=\frac{1}{n^\epsilon}\left[1-\left(1+\frac{c_n}{n}\right)^{-s}\right],$$

it is seen that $a_n n^{1+\epsilon}$ is finite for values of n becoming indefinitely large. Applying the Binomial Theorem, it is

seen that the limit of $a_n n^{1+\epsilon}$ is sc_n. Since $a_n = s\frac{c_n}{n^{1+\epsilon}}$, it follows that $a_1+a_2+a_3+\cdots$ is a convergent series.

Next write $s=s_1+\epsilon$ in the formula (3) and we have

$$\sum \frac{\gamma^s}{n^s} - S = \gamma^s \sum \frac{a_n}{n^{s_1}},$$

which, due to Theorem I, is a finite and continuous function of s_1. When $s_1 = 1-\epsilon$, it is seen that $s=1$, and consequently,

$$\sum \frac{\gamma^s}{n^s} - S = D_s, \tag{4}$$

say, is finite for $s=1$, and in fact becomes

$$D_1 = \sum \frac{\gamma c_n}{n(n+c_n)}.$$

By definition of the Gamma function, we have

$$\Gamma(s) = \int_0^\infty y^{s-1}e^{-y}dy.$$

Writing $nx=y$, it is seen that

$$\frac{1}{n^s} = \frac{1}{\Gamma(s)}\int_0^\infty e^{-nx}x^{s-1}dx.$$

It follows that

$$\sum^n \frac{1}{n^s} = \frac{1}{\Gamma(s)}\int_0^\infty \frac{x^{s-1}e^{-x}dx}{1-e^{-x}}.$$

Since $(s-1)\Gamma(s-1)=\Gamma(s)$, it is seen that

$$\int_0^\infty e^{-x}x^{s-1-1}dx = \Gamma(s-1) = \frac{\Gamma(s)}{s-1}.$$

It follows that

$$\sum \frac{1}{n^s} - \frac{1}{s-1} = \frac{1}{\Gamma(s)}\int_0^\infty x^{s-1}e^{-x}\left(\frac{1}{1-e^{-x}} - \frac{1}{x}\right)dx.$$

The right hand side of this expression is a continuous function for all positive values of s, which becomes for

$s=1$, the Mascheroni-Euler constant [1]

$$\int_0^\infty e^{-x}\left(\frac{1}{1-e^{-x}}-\frac{1}{x}\right)dx=-\Gamma'(1)=0.577215664\cdots.$$

From (4) it follows that

$$D_s=\gamma^s\left(\Sigma\frac{1}{n^s}-\frac{1}{s-1}\right)-\left(S-\frac{\gamma_s}{s-1}\right),$$

and consequently,

$$\operatorname*{Lim}_{s\to 1}\left(S-\frac{\gamma_s}{s-1}\right)=-\gamma\Gamma'(1)-D_1=C_1,$$

as was required in the statement of the theorem.

Applications

The Determination of the Number of Ideal-Classes of a Fixed Realm

Art. 155. In the place of the quantities $\mu_1, \mu_2, \mu_3, \cdots$ of Theorem IV, write the norms of all those ideals of the realm Ω, which norms are not greater than a given positive quantity t, and note that $Z(t)$ denotes the number T of such ideals so that (see formula (ii) under Theorem IV)

$$\text{(1)}\qquad \operatorname*{Lim}_{\rho=1}\Sigma\frac{s-1}{N(\mathfrak{a})^s}=\gamma=\operatorname*{Lim}_{t=\infty}\frac{T}{t},$$

where the summation on the left-hand side is to be taken over all the integral ideals of the realm Ω. These ideals may be distributed (Art. 55) into a finite number of classes, say, $K_1, K_2, \cdots, K_h$; and the problem is to determine h, the number of the ideal-classes.

The ideal $\mathfrak{a}_1$ of a class A_1, say, is characterized through the fact that any ideal i of the reciprocal class when

[1] See Kronecker, *Theorie der einfachen und vielfachen Integrale*, p. 213; also Kronecker, *Zahlentheorie*, p. 318; Goursat, *Traité d'analyse*, Vol. I, p. 42, determines this constant to twenty decimals. See also Serret, *Calcul différentiel et intégral*, 5th Edition, 1900, Vol. II, p. 175; Wilson, *Advanced Calculus*, p. 458, Ex. 13.

multiplied into $\mathfrak{a}_1$ is a principal ideal; and that is,

$$\mathfrak{i}\mathfrak{a}_1 = \alpha\mathfrak{o},$$

where α is an algebraic integer of Ω.

If $\mathfrak{a}_1$ goes through all ideals of the class A_1, then $\mathfrak{i}\mathfrak{a}_1$ goes over all the principal ideals (algebraic integers) which are divisible by $\mathfrak{i}$ and each one only once.

If the norm of $\mathfrak{a}_1$ is not greater than t, then is

$$|N(\alpha)| \leqq |N(\mathfrak{i})|\, t = t_1,$$

say. If T_1 is the number of the ideals of the class A_1 whose norms are not greater than t, then is T_1 also the number of algebraic integers α of Ω, whose norms are not greater than t_1; so that, due to the formula of Art. 153,

$$\operatorname*{Lim}_{t_1 \to \infty} \frac{T_1}{t_1} = \frac{g}{|N(\mathfrak{i})|}, \tag{2}$$

where g, as defined in the article just mentioned, is a constant different from zero and is determined through the nature of the realm Ω.

If $T_2, t_2;\ T_3, t_3;\ \cdots;\ T_h, t_h$ have the same meaning for the classes $A_2, A_3, \cdots, A_h$ as T_1, t_1 have for A_1, it is clear that

$$T = T_1 + T_2 + \cdots + T_h$$

and

$$\frac{T}{t} = \frac{T_1}{t_1}|N(\mathfrak{i}_1)| + \frac{T_2}{t_2}|N(\mathfrak{i}_2)| + \cdots + \frac{T_h}{t_h}|N(\mathfrak{i}_h)|. \tag{2'}$$

From (1) and (2) follows the fundamental formula

$$\operatorname*{Lim}_{s \to 1} \sum \frac{s-1}{N(\mathfrak{a})^s} = gh. \tag{3}$$

The quantity g in this formula is (see formula (1) of Art. 153) supposed known, although its computation depends upon the hypothesis that a fundamental system of units of Ω has been previously determined. When Ω is a realm of order higher than 2, the determination of this

fundamental system of units is of extreme difficulty. Further, the left-hand side of (3) must be computed, a task which has been done in certain special cases only. (Weber, *Algebra*, Vol. II, pp. 724 ff.)

ART. **156.** LEMMA. It may be proved that the infinite product

$$\Pi \frac{1}{1-\frac{1}{p^s}} = \sum_{\nu=1}^{\nu=\infty} \frac{1}{\nu^s} \tag{1}$$

is expressed through the Dirichlet series

$$Z(s) = \prod_p \left[1+\frac{F(p)}{p^s}+\frac{F(p^2)}{p^{2s}}+\frac{F(p^3)}{p^{3s}}+\cdots\right] = \sum_\nu \frac{F(\nu)}{\nu^s},$$

where $F(p^g)$ denotes the number of ideals which have as norms

$$p^g \qquad (g=1, 2, \cdots).$$

For, observe that the principal ideal op admits as factors the finite number of prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_\nu$ of degree, say f_i, where

$$N(\mathfrak{p}_i) = p^{f_i} \qquad (i=1, 2, \cdots, \nu).$$

If then of the factors of the product

$$Z(s) = \prod_{\mathfrak{p}} \frac{1}{1-\frac{1}{N(\mathfrak{p})^s}}, \tag{2}$$

those be collected which have reference to the same prime integer p, the product (2) may be written

$$Z(s) = \prod_p \frac{1}{\left(1-\frac{1}{p^{sf_1}}\right)\left(1-\frac{1}{p^{sf_2}}\right)\cdots\left(1-\frac{1}{p^{sf_\nu}}\right)}, \tag{3}$$

where the multiplication is to be taken over all prime integers. If this product is developed, there is had the sum of all the terms

$$\frac{1}{p^{s(x_1f_1+x_2f_2+x_3f_3+\cdots+x_\nu f_\nu)}} = \frac{1}{N(\mathfrak{p}_1^{x_1}\mathfrak{p}_2^{x_2}\cdots\mathfrak{p}_\nu^{x_\nu})^s}$$

for all integral values x_i which are zero or positive. If further, those of the terms in which $x_1f_1+x_2f_2+\cdots+x_\nu f_\nu$ has the same value μ, say, are united, it is seen that their sum, since every ideal whose norm is p^μ is compounded only of prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, p_\nu$, is nothing other than $\frac{F(p^\mu)}{p^{s\mu}}$. It is then clear that the general term of the product (3) is

$$1+\frac{F(p)}{p^s}+\frac{F(p^2)}{p^{2s}}+\frac{F(p^3)}{p^{3s}}+\cdots.$$

As $F(\nu)$ denotes the number of those ideals $\mathfrak{i}$ whose norms are equal to ν, the Lemma is accordingly proved, when it is shown that the function $F(\nu)$ has the property that for relatively prime arguments a, b there exists the relation

$$F(ab)=F(a)F(b). \tag{4}$$

To prove this let $\mathfrak{i}$ be an ideal for which

$$N(\mathfrak{i})=ab.$$

Since the norm of every ideal factor $\mathfrak{p}$ of $\mathfrak{i}$ can be only the power of a prime integral factor of either a or b, it follows that $N(\mathfrak{p})$ can enter as a factor of only one or the other of these numbers a or b. Hence, $\mathfrak{i}$ is composed of two ideal factors $\mathfrak{a}$ and $\mathfrak{b}$ whose norms consist of the prime factors of a or b. Since

$$ab=N(\mathfrak{i})=N(\mathfrak{a})N(\mathfrak{b}),$$

it follows that $a=N(\mathfrak{a})$ and $b=N(\mathfrak{b})$. Accordingly, there corresponds to every ideal $\mathfrak{i}$ with the norm ab a pair of ideals $\mathfrak{a}$, $\mathfrak{b}$ with the norms a, b. The number of such pairs is $F(a)F(b)$, and vice versa, to every such pair $F(a)F(b)$, since

$$N(\mathfrak{ab})=N(\mathfrak{a})N(\mathfrak{b}),$$

there corresponds an ideal $\mathfrak{i}=\mathfrak{ab}$ whose norm is ab. It follows that the number of such ideals $\mathfrak{i}$ is equal to the

number of the pairs $F(a)$, $F(b)$. And with this is proved the relation (4).

ART. **157.** Using the above lemma, Landau [1] derived as follows the limit

$$\lim_{t=\infty} \frac{T}{t} = \lim_{s=1} (s-1)Z(s), \qquad (s>1),$$

where the Dirichlet zeta-function is,

$$Z(s) = \sum_{\mathfrak{i}} \frac{1}{N(\mathfrak{i})^s}.$$

It is clear for every integral value ν of the positive quantity t that

$$\frac{T}{t} = \frac{F(1)+F(2)+\cdots+F(\nu)}{\nu},$$

and accordingly that

$$(1) \qquad \lim_{t=\infty} \frac{T}{t} = \lim_{\nu=\infty} \frac{F(1)+F(2)+\cdots+F(\nu)}{\nu}.$$

Consider next the different ideals

$$\mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3, \cdots, \mathfrak{i}_k, \cdots$$

arranged according to their norms $N_1, N_2, \cdots, N_k, \cdots$ so that in general

$$N_k \gtreqless N_{k-1}.$$

If then we put $\nu = N_k$, it is seen that the number of those ideals whose norms are $\leqq \nu$ is at least k, since possibly some of the ideals after $\mathfrak{i}_k$, say, $\mathfrak{i}_{k+1}, \mathfrak{i}_{k+2}, \cdots$, have norms $=\nu$. On the other hand, the number of ideals whose norms $\leqq \nu-1$ must be less than k, for the norm of $\mathfrak{i}_k$ is $\nu > \nu-1$.

Accordingly, we have

$$F(1)+F(2)+\cdots+F(\nu-1) < k \leqq F(1)+F(2)+\cdots+F(\nu).$$

[1] Landau, *Crelle's Journal*, Vol. 125, p. 63, and Vol. 127, p. 167. See also Landau, *Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale*, Part II.

It follows at once that

$$(2)\quad \frac{F(1)+F(2)+\cdots+F(\nu-1)}{\nu-1}\cdot\left(1-\frac{1}{\nu}\right)<\frac{k}{N_k} \leqq \frac{F(1)+F(2)\cdots+F(\nu)}{\nu}.$$

Observe in (1) that as $\nu=N_k$ becomes infinite, k also becomes infinite so that (see formulas (2) and (2′), Art. 155)

$$\lim_{t\to\infty}\frac{T}{t}=gh=\lim_{k\to\infty}\frac{k}{N_k}.$$

Next observe that for k a value k' may be chosen so large that for every $k\geqq k'$

$$(3)\quad \frac{gh-\delta}{k}<\frac{1}{N_k}<\frac{gh+\delta}{k}$$

for positive values of δ approaching zero.

Further, note if $s>1$, that

$$Z(s)=\sum_{\mathfrak{i}}\frac{1}{N(\mathfrak{i})^s}=\sum_{k}\frac{1}{N_k^s},$$

and therefore also from (3) that

$$(4)\quad (gh-\delta)^s(s-1)\sum_{k=k'}^{k=\infty}\frac{1}{k^s}<(s-1)\sum_{k=k'}^{k=\infty}\frac{1}{N_k^s} <(gh+\delta)^s(s-1)\sum_{k=k'}^{k=\infty}\frac{1}{k^s}.$$

Since $\sum_{k=k'}^{k=\infty}\frac{1}{k^s}$ for $s>1$, has a finite limit, and as

$$\lim_{s\to 1}(s-1)\sum_{k=1}^{k=\infty}\frac{1}{k^s}=\lim_{s\to 1}(s-1)\sum_{k=k'}^{k=\infty}\frac{1}{k^s}=1,$$

it follows, when s approaches 1 in (4), that

$$gh-\delta<\lim_{s\to 1}(s-1)Z(s)<gh+\delta.$$

Hence, as $\delta\to 0$, it is seen that

$$(5)\quad \lim_{s\to 1}(s-1)Z(s)=gh=\lim_{t\to\infty}\frac{T}{t},$$

as was to be proved.

But as noted in Art. 155, end, the above may be considered only as a starting point for the solution of the general case. It offers important conclusions regarding the nature of the number of classes.

The following transformations [1] may prove useful in many cases. Put

$$\sum \frac{1}{N(\mathfrak{a})^s} = \Phi(s). \tag{6}$$

Further, let $\mathfrak{p}$ be any prime ideal of the fth degree in Ω, so that

$$N(\mathfrak{p}) = p^f$$

(Art. 29); and observe that

$$1 + \frac{1}{N(\mathfrak{p})^s} + \frac{1}{N(\mathfrak{p})^{2s}} + \cdots = \frac{1}{1 - N(\mathfrak{p})^{-s}} = \frac{1}{1 - p^{-sf}}.$$

If such series for all the different prime ideals be multiplied together, it is clear that there results a sum of terms, each of the form

$$\left(\frac{1}{N(\mathfrak{p})^k} \frac{1}{N(\mathfrak{p}_1)^{k_1}} \frac{1}{N(\mathfrak{p}_2)^{k_2}} \cdots\right)^s = \frac{1}{N(\mathfrak{p}^k \cdot \mathfrak{p}_1^{k_1} \cdot \mathfrak{p}_2^{k_2} \cdots)^s}.$$

All such terms are of the form $N(\mathfrak{a})^{-s}$, each term appearing once and only once. And from (6) it is evident that

$$\Phi(s) = \Pi \frac{1}{1 - N(\mathfrak{p})^{-s}}.$$

Let $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_e$ be the different prime factors of p, each being respectively of the degree $f_1, f_2, \cdots, f_e$. We then have

$$\Phi(s) = \overset{p}{\Pi} \frac{1}{(1 - p^{-sf_1})(1 - p^{-sf_2}) \cdots (1 - p^{-sf_e})}, \tag{7}$$

where the product is to be taken over all rational prime integers p.

[1] Weber, *Algebra*, Vol. II, p. 723.

From (3) it is seen [1] that

$$gh = \lim_{s \to 1} (s-1)\Phi(s). \tag{8}$$

There exist many important applications of this formula. Observe that

$$1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\cdots=\frac{1}{1-p^{-s}}.$$

If the product of this expression is taken for all prime integers, it is clear that

$$\prod^{p}\frac{1}{1-p^{-s}}=\sum^{n}\frac{1}{n^s}, \tag{9}$$

where the summation on the right is taken over all rational integers. The product on the left has a finite value for all values of s which are greater than 1. Since the right-hand side of this expression is a convergent series, it follows also that the reciprocal value, namely, the product

$$P=\prod^{p}(1-p^{-s}),$$

each of whose factors being less than unity, has a value that is different from zero, so long as $s>1$. This property is also, of course, true if in the formation of the product P only a part of all the prime numbers p are taken into consideration, the product being thereby increases without becoming greater than unity.

From this it appears that in the product (7), the partial product

$$\prod\frac{1}{1-p^{-sf}}$$

which is taken over all prime integers p, for which $f>1$, is also finite for $s=1$. And on the other hand since g and h have definite values, that are different from zero, we have from (9) the important theorem:

[1] See also for example, Hilbert's *Bericht*, etc., p. 230.

THEOREM. *If* $\mathfrak{p}$ *goes over all prime ideals of the first degree of an algebraic realm* Ω, *the product*

$$(s-1)\Pi\frac{1}{1-N(\mathfrak{p})^{-s}}$$

has as $s\to 1$ *a finite limit which is different from zero.* It appears from this formula that *in every algebraic realm there are an infinite number of prime ideals of the first degree.*

Remark. In this connection read Dirichlet, "Recherches sur diverses applications, etc.," *Crelle*, Vol. 19, p. 324; Vol. 21, pp. 1 and 134; *Werke*, Vol. I, p. 411; Dirichlet, "Recherches sur les formes quadratiques, etc.," *Crelle*, Vol. 24, p. 291; *Werke*, Vol. I, p. 533. For other references and illustrative examples see Dedekind, "Ueber die Anzahl der Idealklassen in reinen kubischen Zahlkörpern," *Crelle*, Vol. 121, pp. 121 ff. See also Hecke, *Theorie der algebraischen Zahlen*, § 51.

ART. **158. Fundamental Theorem.** *In every ideal class there is an ideal whose norm is not greater than the absolute value of the square root of the discriminant of the realm.* (Minkowski, *Werke*, Vol. I, p. 258.)

Continuing the heading "Applications" of p. 313, we shall prove anew this theorem and give certain consequences of it. (See also Arts. 137 and 149.)

Proof. Let A be an arbitrary ideal class and let $\mathfrak{i}$ be an ideal of the reciprocal class. Then (Vol. I, Arts. 218 and 309) there is an integer in Ω, say ι, which is divisible by $\mathfrak{i}$ and is such that

$$|N(\iota)| \leqq N(\mathfrak{i})\,|\sqrt{D}|.$$

Since ι is divisible by $\mathfrak{i}$, write

$$\iota = \mathfrak{i}\mathfrak{a},$$

where $\mathfrak{a}$ belongs to the class A (Vol. I, Art. 309). Hence,

$$N(\iota) = N(\mathfrak{i})N(\mathfrak{a}),$$

and consequently

$$N(\mathfrak{a}) \leqq |\sqrt{D}|.$$

Further, observe that there are only a finite number of rational integers that are less than or equal to $|\sqrt{D}|$ and these offer as factors only a finite number of different ideals. And from this follows the important theorem.

THEOREM. *There are only a finite number of ideal classes of* Ω. (Dirichlet-Dedekind, *Zahlentheorie*, pp. 603 ff., and Kronecker, *Grundzüge*, p. 64.)

The above theorem offers a simple method of finding through a finite number of operations, a complete system of non-equivalent ideals for a given realm. For, we need consider only those ideals whose norms $\leqq |\sqrt{D}|$. To determine among such ideals those that are equivalent, take each one of them and multiply it respectively by each of the others. If $\mathfrak{i}$ denotes any such product, determine in $\mathfrak{i}$ a number ι whose norm in absolute value has the least value and observe whether $\mathfrak{i} = (\iota)$. And that is, whether $\mathfrak{i}$ consists of two factors that belong to reciprocal classes.

Note (as above) that if $\mathfrak{a}$ is any ideal there is always an integer α divisible by $\mathfrak{a}$ and such that

$$|N(\alpha)| \leqq N(\mathfrak{a})\,|\sqrt{D}|.$$

If further $\iota_1, \cdots, \iota_n$ form a basis of $\mathfrak{i}$, it is only necessary to determine $u_1, \cdots, u_n$ as rational integers which do not all vanish and in such a way that the real and imaginary parts of

$$u_1\iota_1^{(s)} + \cdots + u_n\iota_n^{(s)} \qquad (s = 1, \cdots, n)$$

remain within certain fixed limits. And that requires a finite number of operations. In the same way it is clear that for any given ideal the class to which it belongs may be determined through a finite number of operations. Recurrent computations of the class number h in

cyclotomic realms, whose degrees are powers of 2, are found in Weber's *Algebra*, Vol. II, pp. 784 ff. If the degree of the realm is $n=2^k$, Weber shows (p. 802) that one of the factors A_k of h has values 1, 17, 21121 for values $k=5$, 6, 7, respectively. For the class number in quadratic realms, see Hilbert, *Bericht*, p. 318; and Derichlet, *Werke*, Vol. I, pp. 357 and 411.

ART. **159. A System of Fundamental Classes.** It has been shown that the number of ideal classes is finite ($=h$). These classes form a *finite group* of degree h (Art. 55), since the product of two of the classes is a class. The multiplication of the classes as also of the ideals, is a commutative as well as an associative process.

Since the h power of every class C is equal to the principal class (Art. 55), there must exist a smallest positive power c, say, of C, such that C^c is identical with the principal class. It is also clear that c is a divisor of h (Art. 39, and Vol. I, Art. 198). Suppose that the smallest exponent to which each class *belongs* (Vol. I, Art. 224) has been determined. Let h_1 be the greatest of these exponents and let K_1 be one of the classes to which h_1 belongs, so that

$$K_1^{h_1}=H,$$

where H is the principal class.
It is clear that the powers

$$K_1,\ K_1^2,\ \cdots,\ K_1^{h_1} \tag{1}$$

are all different classes. If $h=h_1$, all the classes are found in the series (1); if, however, $h>h_1$, there are other classes of ideals not included in (1).

The exponent h' to which any other class C belongs must be a divisor of h_1; for, on the assumption that this were not true, the least common multiple of h_1 and h' would be greater than h_1. Distribute this least common

multiple into two factors $\lambda_1 \cdot \lambda'$, where λ_1 and λ' are relatively prime and are, respectively, divisors of h_1 and h'. Observe then that the product

$$K_1^{\frac{h_1}{\lambda_1}} \cdot C^{\frac{h'}{\lambda'}}$$

is a class which belongs to the exponent $\lambda_1\lambda'$, where $\lambda_1\lambda'$ is greater than h_1 contrary to the assumption.

Observe next that for every class C there is a smallest positive power k, say, such that C^k is equal to one of the classes $K_1, K_1^2, \cdots, K_1^{h_1}$; for, if there is no other, then clearly $C^{h'} = H = K_1^{h_1}$, where H is the principal class. Also note that h' must be a divisor of h_1.

Suppose that such an exponent has been derived for every class. Let h_2 be the greatest among these new exponents and let K_2 be one of the classes which must be raised to the h_2 power in order that

$$K_2^{h_2} = K_1^s,$$

where s is one of the integers $1, 2, \cdots, h_1$.

Next form the classes

$$K_1^{x_1} \cdot K_2^{x_2} \quad (x_1 = 1, 2, \cdots, h_1;\ x_2 = 1, 2, \cdots, h_2) \tag{2}$$

and observe that they are all different. For, suppose that

$$K_1^{x_1} \cdot K_2^{x_2} = K_1^{y_1} \cdot K_2^{y_2},$$

where y_1 is one of the integers $1, 2, \cdots, h_1$, and y_2 is one of the integers $1, 2, \cdots, h_2$.

It follows that

$$K_1^{x_1 - y_1} = K_2^{y_2 - x_2}$$

where, due to the fact that

$$K_2^{h_2} = K_1^{s_1},$$

it would follow that we may take as the exponent of K_2 a positive integer k_2 less than h_2, and such that

$$K_2^{k_2} = K_1^{s_1} \qquad (s_1 \leqq h_1),$$

contrary to the definition of h_2 and K_2.

It is seen that the exponents to which any new class belongs must be a divisor of h_2.

It is further seen that every such class C when raised to a definite positive power is equal to one of the classes (2). Let these least positive powers be determined and let h_3 be the greatest among them, and let K_3 be one of the classes which belongs to h_3. It is clear that the products

$$K_1^{x_1}K_2^{x_2}K_3^{x_3} \qquad \begin{Bmatrix} x_1=1, 2, \cdots, h_1 \\ x_2=1, 2, \cdots, h_2 \\ x_3=1, 2, \cdots, h_3 \end{Bmatrix} \tag{3}$$

offer $h_1 \cdot h_2 \cdot h_3$ different classes. The exponents to which the remaining classes belong, must be divisors of h_3. Continuing, it is seen that there are certain classes $K_1, K_2, \cdots, K_\sigma$, such that every class is presented and only once through the product

$$K_1^{x_1} \cdot K_2^{x_2} \cdots K_\sigma^{x_\sigma}, \tag{i}$$

if the x's are permitted to take respectively rational integral values up to $h_1, \cdots, h_\sigma$, these h's being certain positive integers.

Due to the method by which $K_1, \cdots, K_\sigma$ have been determined, it is seen that

$$K_i^{h_i} = K_{i-1}^{a_{i-1}} \cdot K_{i-2}^{a_{i-2}} \cdots K_1^{a_1}, \tag{4}$$

where $a_{i-1}, \cdots, a_1$ are positive integers or zero.

Observe that

$$K_{i-1}^{h_{i-1}} = K_{i-2}^{b_{i-2}} \cdot K_{i-3}^{b_{i-3}} \cdots K_1^{b_1},$$

where the b's are also positive integers or zero. And, since the exponent of any other class when expressed as a product of powers of $K_{i-2}, \cdots, K_1$ is a divisor of h_{i-1}, it is clear that any new class raised to the power h_{i-1} may be expressed as a product of the classes $K_{i-2}, \cdots, K_1$ and therefore also $K_i^{h_{i-1}}$ may be expressed as a product of these classes in the form

$$K_i^{h_{i-1}} = K_{i-2}^{c_{i-2}} \cdot K_{i-3}^{c_{i-3}} \cdots K_2^{c_2} \cdot K_1^{c_1}. \tag{5}$$

It follows that h_i must be a divisor of h_{i-1}; for, otherwise

$$h_{i-1} = h_i q + r,$$

where q is an integer and $0 < r < h_i$, and therefore

$$K_i^{h_{i-1}} = (K_i^{h_i})^q K_i^r$$

and consequently from (4) and (5), K_i^r may be expressed as a product of the classes $K_{i-1}, \cdots, K_1$, which, since $r < h_i$ is in contradiction with the definition of h_i and K_i.

We may therefore write $h_{i-1} = h_i l$, where l is an integer, and from (4) it follows that

$$K_{i-1}^{l \cdot a_{i-1}}$$

may be expressed as a product of classes $K_{i-2}, \cdots, K_1$; and as h_{i-1} is by definition the lowest power of K_{i-1} which can be expressed through a product of these classes, it follows also that $l \cdot a_{i-1}$ is divisible by h_{i-1} and that is, by $h_i l$, so that a_{i-1} is divisible by h_i.

Put $a_{i-1} = h_i c_i$ and write

$$C_i = K_i K_{i-1}^{-c_i} \qquad \text{or} \qquad K_i = C_i K_{i-1}^{c_i}. \tag{6}$$

It follows from (4) that

$$C_i^{h_i} = K_{i-2}^{a_{i-2}} \cdot K_{i-3}^{a_{i-3}} \cdots K_1^{a_1}. \tag{7}$$

Observe further that due to the relation (6), the class C_i may be substituted in formula (i) above in the place of K_i and since

$$K_i^{h_i} = C_i^{h_i} K_{i-1}^{c_i h_i},$$

it is seen that $C_i^{h_i}$ like $K_i^{h_i}$ may be expressed as a product of powers of $K_{i-1}, K_{i-2}, \cdots, K_1$. It is also clear that all the classes in Ω may still be represented through the formula (i) after the substitution of C_i for K_i in it, since C_i belongs to the same exponent h_i as K_i.

We may then continue in the same manner with formula (7) as was done with (4), it being evident that K_i may be replaced eventually through a class A_i such

that

$$A_i^{h_i}=H,$$

where H is the principal class. And this may be expressed in the form of the theorem:[1]

THEOREM. *There are certain fundamental classes* $A_1, \cdots, A_\sigma$ *such that* $A_i^{h_i}=H$ $(i=1, 2, \cdots, \sigma)$, *and through which every class* C *may be expressed once and only once in the form*

$$C=A_1^{x_1}\cdots A_\sigma^{x_\sigma}, \tag{8}$$

where $x_1, \cdots, x_\sigma$ *go through all integers respectively from* 1 to h_1, 1 to h_2, $\cdots$, 1 to h_σ. *And further*

$$h=h_1\cdot h_2\cdots h_\sigma, \tag{9}$$

where each h *is a divisor of the preceding.*

It is possible to replace formula (8) by another which may offer peculiar advantages. Suppose that h_i when decomposed into its prime factors is

$$h_i=p'\cdot p''\cdot p'''\cdots, \tag{10}$$

where the p's are prime integers or powers of primes. We may then determine uniquely the integers a', a'', a''', $\cdots$, so that

$$\frac{1}{h_i}=\frac{a'}{p'}+\frac{a''}{p''}+\frac{a'''}{p'''}+\cdots,$$

where

$$0<a'<p',\ 0<a''<p'', \text{ etc.}$$

It is seen that

$$A_i^{x_i}=(A_i^{\frac{h_i}{p'}})^{a'x_i}(A_i^{\frac{h_i}{p''}})^{a''x_i}\cdots;$$

or, if we put

$$A_i^{\frac{h_i}{p'}}=B_i',\ A_i^{\frac{h_i}{p''}}=B_i'',\ \cdots,$$

it follows that

$$A_i^{x_i}=B_i'^{a'x_i}\cdot B_i''^{a''x_i}\cdots.$$

[1] In the derivation of this theorem the method has been followed that is found in Bachmann, *Allgemeine Arithmetik*, pp. 377 ff.

Observe that the classes B_i', B_i'', $\cdots$ satisfy the equations

$$B_i'^{p'} = H, \quad B_i''^{p''} = H, \quad \cdots.$$

It is thus seen that every ideal class may be uniquely expressed through a series of new fundamental classes which *belong* to exponents that are prime integers or powers of such integers. And that is, the classes, when raised to such primes as exponents, are themselves equal to the principal class.

Observe, however, that, although we have gained a certain simplicity in the above expressions, we have lost a fundamental property of the h's of formula (9), which formula expressed that every h was a divisor of the preceding h. However, formulas (9) and (10) tell us that in the latter representation of the ideal classes the product of all the exponents to which the new fundamental classes belong remains equal to the number h of the ideal classes.[1]

ART. **160. A Retrospect and a Prospect.** Hensel ("Untersuchung der Fundamental-Gleichung einer Gattung für eine realle Primzahl als Modul, etc.," *Crelle's Journal*, Vol. 113, p. 85), writes: "If

$$p = \mathfrak{p}_1^{\delta_1}\mathfrak{p}_2^{\delta_2}\cdots\mathfrak{p}_h^{\delta_h}$$

is the factorization of the prime integer p into its prime ideal factors, and if

$$N(\mathfrak{p}_1\cdot\mathfrak{p}_2\cdots\mathfrak{p}_h) = p^r$$

is the norm of the product of all the different prime factors, then is the discriminant of the algebraic stock-realm exactly divisible by

$$p^{n-r}$$

and by no higher power of p."

[1] Kronecker, *Werke*, Vol. I, p. 271; Hilbert, *Bericht*, p. 233; Schering, *Gött. Abh.* 14, 1869.

Here as in Art. 92 there exist the relations

$$k_1\delta_1+k_2\delta_2+\cdots+k_h\delta_h=n,$$

and

$$k_1+k_2+\cdots+k_h=r,$$

n being the degree of the algebraic realm.

An exception enters in the case where one of the exponents δ is divisible by p. In this exceptional case the power p^{n-r} is *not* the highest power of p that divides the discriminant. Such prime numbers p for which there exist these special cases are called "Singular primes," Art. 108, and are treated in the last chapter of the present work.

The following is a corollary of the above theorem:

A prime integer p is then and only then a divisor of the discriminant, if in the given realm p is factorable in one or more equal ideal factors. For the discriminant may be written

$$D(u_1, u_2, \cdots, u_n) = p^{k_1(\delta_1-1)+k_2(\delta_2-1)+\cdots+k_h(\delta_h-1)}H(u_1, u_2, \cdots, u_n),$$

where H is a form that is relatively prime to p; and it is clear that the integer $n-r$ is different from zero only when at least one of the exponents δ is greater than unity. From this it is seen that within any algebraic realm there exists only a limited number of prime integers, which have equal factors, these being the divisors of the discriminant. All the other prime integers in the given realm have only different (and not equal) prime factors. The proof of the above theorem was one of the great advances due to Dedekind, "Ueber die Discriminanten endlicher Körper," *Abh. d. Königlichen Gesellschaft der Wissenschaften zu Gottingen*, Vol. 29; *Werke*, Vol. I, p. 351.

The Dedekind method of procedure is characterized by Hensel as follows: "Dedekind sought to establish a

theory of algebraic numbers whereby in the place of the fundamental form ξ of Art. 71, which may be correctly regarded as an invariant of all algebraic integers in the fixed realm, he made fundamental (see Art. 92) a special quantity $\gamma = a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n$, and that is, in the place of the indeterminates $u_1, u_2, \cdots, u_n$ of the fundamental form, Dedekind wrote rational integers $a_1, a_2, \cdots, a_n$. He then sought to determine the congruence (mod. p) of lowest possible degree which γ satisfied, the degree being the same as in the congruence satisfied by the fundamental form."

This can be the case (see Art. 92) only if the determinant

$$|U_{gh}| = \theta(u_1, u_2, \cdots, u_n),$$

which for the indeterminates $u_1, u_2, \cdots, u_n$ is *not* divisible by p, is also *not* divisible by p for $u_1 = a_1, u_2 = a_2, \cdots, u_n = a_n$. However, examples are not hard to find (see Art. 99), in which the above determinant is divisible by p, when the u's are replaced by *any* system of rational integers. And consequently, Hensel insists, the above theorem cannot be proved in so simple a manner, if one, neglecting the theory of integral forms, confines himself only to algebraic integers. However, as indicated by Hensel, Dedekind in a most ingenious (*Scharfsinnig*) manner overcame this difficulty in that he proved that the discriminant of the realm is the norm of an ideal, whose prime ideal factors are also determined. The treatment of this *fundamental ideal* (*Grundideal*) of Dedekind, which is the *different* (Hilbert) of the fundamental form (Kronecker), and in particular the determining of its ideal factors, is made paramount in the discussions which follow. Observe that the norm of this different is the discriminant of Kronecker's fundamental

equation. The derivation of these results, Hensel regards as the most beautiful, although the most difficult, of the whole Dedekind theory. Hensel further insists that the theory of algebraic forms as founded by Kronecker leads to the desired results in a more straightforward and simpler manner. And it is eqally true that this theory has guided Professor Hensel in his own epoch-making researches in the arithmetical solution of algebraic equations.

It may be remarked, says Hensel, that the indeterminate coefficients $u_1, u_2, \cdots, u_n$ of the fundamental form ξ have *not* been introduced into the investigation through formal grounds (*Gründe*); their introduction is necessary and sufficient that the fundamental form, when specialized, offer all the integers of the algebraic realm and that the fundamental equation offer all the integral equations.

The prime factors $\mathfrak{p}$ of p are had through the factorization of the fundamental equation into its irreducible factors, modulo p. These prime factors are presented through

$$\text{(a)} \qquad \mathfrak{p}_h = p + F_h(\xi; u_1, u_2, \cdots, u_n);$$

and are consequently forms, whose indeterminates are intimately connected with the question, when the Kronecker theory is applied to a definite problem. But, says Hensel, the essential point in the Kronecker theory consists in the fact that only the system of algebraic integers $p, \xi^{(1)}, \xi^{(2)}, \cdots$ are of importance, which are the coefficients of the products of the powers of the u's in the expansion of $F_h(\xi; u_1, \cdots, u_n)$, so that the expression (a) may well be replaced by a linear form

$$p + v^{(1)}\xi^{(1)} + v^{(2)}\xi^{(2)} + \cdots,$$

where now the v's are the indeterminates.

Thus, in the general theory of the divisors as given in Kronecker's *Festschrift*, the independence of the divisors of the special choice of the indeterminates is insisted upon. But we are not to conclude that these indeterminates have nothing to do with any individual problem; in fact, in every investigation the indeterminates stand in the closest and most necessary relation to the problem that is being treated. Kronecker's aim was to develop a theory which included as special cases the ideal numbers of Kummer and the moduls and ideals of Dedekind. With this in view he made his given algebraic realm a sub-realm of a Galois realm and the resolvents in this realm he wished to treat in all their generality by means of modular (divisor) systems of the second, third, and higher kinds. To complete the theory of the individual special orders (Arten) of algebraic numbers, Kronecker wished to transfer the equivalence (*Aequivalenz-Bestimmung*), which Kummer had employed for his *ideal divisors*, to these real (*wirklichen*) algebraic divisors (see *Festschrift*, p. 63).

In Vol. I, Art. 205, was given a notion of Kummer's *Aequivalenz-Bestimmung* for his *ideal* divisors. This concept generalized with Kronecker is the " Principle of the association of new structures of quantities (*Grössengebilde*) with a given realm of integers and order-modul or Species (*Festschrift*, p. 48) of integers therein."

It would appear that the " very source of a new light " with Kronecker (*Festschrift*, p. 32) is what he calls the Galois " Algebraic Principle." By making any algebraic realm $\mathfrak{k}$ a sub-realm of a Galois realm $\mathfrak{R}$ he was able to apply a " Principle of the Association of new structures of quantities (*Grössengebilde*) to integers, order-moduls, etc. of the realm $\mathfrak{R}$; and whereas Kummer (see Kronecker's *Festschrift*, p. 48) introduced a sort of equivalence

of so-called *ideal-divisors* (=mental concepts) for algebraic numbers in certain special algebraic realms, Kronecker wished to transfer such an equivalence of algebraic numbers, order-moduls, etc. in any algebraic realm $\mathfrak{k}$ to the *real* (and no longer fictitious) algebraic divisors in $\mathfrak{R}$ (*Festschrift*, p. 63), and with this it was Kronecker's aim to develop a theory which included as special cases the "ideal numbers" of Kummer and the ideals of Dedekind. Proceeding along these lines he encountered difficulties, which he himself (see Introduction to Vol. I) never succeeded in overcoming. This work his genial pupil Hensel has so efficiently and effectively carried on.

The author believes that Hilbert's Work on Galois Realms (*Bericht*, Chapter XV) will prove exceedingly helpful in the further development of the Kronecker Theory. Bachmann, following the Dedekind method of approach, worked out this theory of Hilbert more in detail and this is reproduced in Chapter XV of the present work. H. Weber, employing the Kronecker Theory of Forms, has given these results a more general form as is indicated in Chapter XIV. And thus the prospect for the further development of mathematical theories along the lines here indicated, seems very fruitful.

CHAPTER X

THE ORDER-MODULS

ART. **161.** It has been seen that in every algebraic realm there exists an order-modul $\mathfrak{o} = [\omega_1, \omega_2, \cdots, \omega_n]$, such that all integers of the realm may be expressed linearly through $[\omega_1, \omega_2, \cdots, \omega_n]$ with rational integral coefficients. It was seen further that $\mathfrak{o}$ satisfied the relations

$$\mathfrak{o}\mathfrak{o} = \mathfrak{o} \qquad \text{and} \qquad \frac{\mathfrak{o}}{\mathfrak{o}} = \mathfrak{o}.$$

(Vol. I, Art. 133.) Mention has been made of order-moduls $\mathfrak{o}_1$ in $\mathfrak{o}$, and that is, of moduls consisting of n integers of the realm in which moduls are found all the rational integers and for which there exists the relation [1]

$$\mathfrak{o}_1\mathfrak{o}_1 = \mathfrak{o}_1 \qquad \text{and} \qquad \frac{\mathfrak{o}_1}{\mathfrak{o}_1} = \mathfrak{o}_1$$

(Art. 104).

We also saw (Art. 104) that $\frac{\mathfrak{o}_1}{\mathfrak{o}} = \mathfrak{f}$, where $\mathfrak{f}$ is the ring-leader of $\mathfrak{o}_1$ and that $\mathfrak{o}\mathfrak{f} = \mathfrak{f}$. It follows that $\mathfrak{f}$ is an ideal in the given realm. We further have the additional relations

$$\mathfrak{f} > \mathfrak{o}_1, \qquad [1] > \mathfrak{o}_1 \qquad \text{and} \qquad \mathfrak{o}\mathfrak{o}_1 = \mathfrak{o}.$$

Another definition of the order-modul due to Dedekind (*Werke*, Vol. I, pp. 124 ff.) may be noted here:

Let $\theta_1, \theta_2, \cdots, \theta_k$ be any integers of an algebraic realm through which the realm is completely determined; and

[1] See Dedekind, *Festschrift zur Säkularfeier der Geburstages von Carl Friederich Gauss*, Braunschweig, 1877; and Bachmann, *Allgemeine Arith.*, etc., pp. 360 et seq.

that is, on the one hand, every number of the realm must be expressed rationally through these quantities with integral coefficients or, on the other hand, integrally through these quantities with rational coefficients. The corresponding realm of integrity (the realm which contains all integers that may be expressed through these quantities) contains the modul [1], consisting of all rational integers, and is such that its integers when multiplied together, again produce integers of the realm of integrity. More definitely, it is an order-modul in $\mathfrak{o}$. For, let

$$\mathfrak{o}_1 = [\alpha_1, \alpha_2, \cdots, \alpha_k] \tag{1}$$

be such a modul in its reduced form. As every number of the fixed realm may be expressed integrally through $\alpha_1, \alpha_2, \cdots, \alpha_k$ with rational coefficients, it follows that the basal elements $\omega_1, \omega_2, \cdots, \omega_n$ of $\mathfrak{o}$, when multiplied by suitably chosen rational integers g_i, may be expressed in the form

$$g_i\omega_i = a_{i1}\alpha_1 + a_{i2}\alpha_2 + \cdots + a_{ik}\alpha_k \quad (i=1, 2, \cdots, n),$$

where a_{ik} are rational integers. From this it may be proved that $k=n$; and that consequently the modul (1) is an n-termed modul consisting of algebraic integers of the realm. This modul has the property of an order-modul. (See Arts. 3, 4, and 9.)

From this it is seen also that an order-modul $\mathfrak{o}_1$ in $\mathfrak{o}$ may be defined as any realm of integrity through whose integers the fixed realm of rationality is produced.

ART. 162. The concept of an ideal $\mathfrak{i}$ in $\mathfrak{o}_1$ is the analogue of that of an ideal in $\mathfrak{o}$ (Art. 3). And that is, it may be defined as a modul in $\mathfrak{o}_1$ such that

$$\mathfrak{o}_1\mathfrak{i} > \mathfrak{i}. \tag{1}$$

Since the modul [1] is contained in $\mathfrak{o}_1$, the inequality (1)

is in fact the equality

$$\mathfrak{o}_1\mathfrak{i}=\mathfrak{i}, \tag{2}$$

since $\mathfrak{i}>\mathfrak{o}_1\mathfrak{i}$.

Hilbert [1] calls such ideals "ring-ideals." It follows from the preceding article that every ideal $\mathfrak{i}$ in $\mathfrak{o}_1$ is an n-termed modul. In other words, such an ideal consists of n integers, say $\tilde{\omega}_1, \tilde{\omega}_2, \cdots, \tilde{\omega}_n$ of the fixed realm. And, since $\mathfrak{i}$ is divisible by $\mathfrak{o}_1$, it is seen that the least common multiple of $\mathfrak{i}$ and $\mathfrak{o}_1$ is $\mathfrak{i}$. Accordingly, we have

$$\mathfrak{o}_1-\mathfrak{i}=\mathfrak{i}.$$

Further, if the basal elements of this least common multiple are $\mu_1, \mu_2, \cdots, \mu_n$, it follows from Vol. I, Art. 93 that

$$\mu_i=a_{i1}\tilde{\omega}_1+a_{i2}\tilde{\omega}_2+\cdots+a_{in}\tilde{\omega}_n \quad (i=1, 2, \cdots, n),$$

where the a's are rational integers. The determinant of these linear forms offers the number of classes of incongruent numbers into which the integers of the order-modul $\mathfrak{o}_1$ may be distributed with respect to the ideal $\mathfrak{i}$. This number is symbolically denoted by

$$|a_{ik}|=(\mathfrak{o}_1, \mathfrak{i}),$$

where the positive sign of the determinant is to be taken. Following the analogy of the definition of the norm of a realm ideal, we may define the above number as the *norm* of the ideal $\mathfrak{i}$, which belongs to the order-modul $\mathfrak{o}_1$. It is denoted by $N'(\mathfrak{i})$. (Arts. 11 and 19.)

ART. **163.** We shall denote in this chapter the realm ideals by $\mathfrak{j}$ and use $\mathfrak{i}$ to denote the ideals of an order-modul. Observe that the ring-leader $\mathfrak{f}_0$ of $\mathfrak{o}$ is $\mathfrak{o}$ and that

$$\mathfrak{j}+\mathfrak{f}_0=\mathfrak{j}+\mathfrak{o}=\mathfrak{o} \qquad \text{where} \qquad \frac{\mathfrak{o}}{\mathfrak{o}}=\mathfrak{f}_0.$$

We shall in a somewhat restricted sense limit the concept

[1] Hilbert, *Bericht über alg. Zahlkörper*, p. 237.

of an ideal in $\mathfrak{o}_1$ through the definition [1]

$$\mathfrak{i}+\mathfrak{f}=\mathfrak{o}_1, \qquad \text{where} \qquad \frac{\mathfrak{o}_1}{\mathfrak{o}}=\mathfrak{f}.$$

With this definition it follows (Vol. I, Art. 143) that, if α and β are any two integers of $\mathfrak{o}_1$, the two congruences

$$\tilde{\omega}\equiv\alpha \pmod{\mathfrak{i}}, \qquad \tilde{\omega}\equiv\beta \pmod{\mathfrak{f}}$$

may always be satisfied by an integer $\tilde{\omega}$ in $\mathfrak{o}_1$.

Using this definition of an ideal in $\mathfrak{o}_1$, we may prove that *the order-modul of every ideal* $\mathfrak{i}$ *in* $\mathfrak{o}_1$ *is* $\mathfrak{o}_1$. (For the analogue of this theorem in $\mathfrak{o}$, see Art. 4.)

Observe that the order-modul $\mathfrak{i}^0$ of $\mathfrak{i}$ is the complex of all integers γ for which $\gamma\mathfrak{i}>\mathfrak{i}$. Due to the relation $\mathfrak{o}_1\mathfrak{i}>\mathfrak{i}$, it follows that

(1) $$\mathfrak{o}_1>\mathfrak{i}^0.$$

Further, since

$$[1]>\mathfrak{i}^0>\mathfrak{o}, \qquad [1]\mathfrak{f}=\mathfrak{f}, \qquad \text{and} \qquad \mathfrak{o}\mathfrak{f}=\mathfrak{f},$$

it follows that

$$\mathfrak{f}>\mathfrak{i}^0\mathfrak{f}>\mathfrak{f},$$

so that

(2) $$\mathfrak{i}^0\mathfrak{f}=\mathfrak{f}.$$

By definition

$$\mathfrak{i}+\mathfrak{f}=\mathfrak{o}_1, \qquad \text{or} \qquad \mathfrak{i}\mathfrak{i}^0+\mathfrak{f}\mathfrak{i}^0=\mathfrak{o}_1\mathfrak{i}^0.$$

Since $\mathfrak{i}\mathfrak{i}^0=\mathfrak{i}$, it follows, from the definition of $\mathfrak{i}$ in $\mathfrak{o}_1$ that

$$\mathfrak{o}_1\mathfrak{i}^0=\mathfrak{i}+\mathfrak{f}=\mathfrak{o}_1.$$

Since $[1]>\mathfrak{o}_1$, it is further seen that

(3) $$\mathfrak{i}^0>[1]\mathfrak{i}^0>\mathfrak{o}_1\mathfrak{i}^0=\mathfrak{o}_1.$$

From (1) and (3) we have

$$\mathfrak{i}^0=\mathfrak{o}_1.$$

ART. **164.** It may be proved next that the greatest common divisor $\mathfrak{i}'+\mathfrak{i}''$, the least common multiple $\mathfrak{i}'-\mathfrak{i}''$, the product $\mathfrak{i}'\mathfrak{i}''$ of two ideals $\mathfrak{i}'$ and $\mathfrak{i}''$ in $\mathfrak{o}_1$ are ideals in $\mathfrak{o}_1$.

[1] Hilbert, *op. cit.*, p. 243, makes a mistake in this connection which he remedies on p. 537. He called such ideals "regular ring-ideals."

The first condition, namely, that $\mathfrak{o}_1\mathfrak{i}=\mathfrak{i}$ is evidently true for the three cases. The second condition, namely $\mathfrak{f}+\mathfrak{i}=\mathfrak{o}_1$, may be proved for the three cases as follows:

First,

$$(\mathfrak{i}'+\mathfrak{i}'')+\mathfrak{f}=\mathfrak{i}'+(\mathfrak{i}''+\mathfrak{f})=\mathfrak{i}'+\mathfrak{o}_1=\mathfrak{o}_1.$$

Secondly, due to the relation $\mathfrak{i}+\mathfrak{f}=\mathfrak{o}_1$, it follows that

$$\mathfrak{o}_1\mathfrak{i}''=\mathfrak{i}'\mathfrak{i}''+\mathfrak{f}\mathfrak{i}''. \tag{1}$$

Since $\mathfrak{i}'\mathfrak{i}''>\mathfrak{o}_1\mathfrak{i}'=\mathfrak{i}'$, and $\mathfrak{i}'\mathfrak{i}''>\mathfrak{o}_1\mathfrak{i}''=\mathfrak{i}''$, it is seen that the complex $\mathfrak{i}'\mathfrak{i}''$ is found in both $\mathfrak{i}'$ and $\mathfrak{i}''$, and therefore also in their least common multiple $\mathfrak{m}=\mathfrak{i}'-\mathfrak{i}''$. Next observe that

$$\mathfrak{i}\mathfrak{f}>\mathfrak{o}\mathfrak{f}=\mathfrak{f}.$$

It follows from (1) that

$$\mathfrak{i}''>\mathfrak{m}+\mathfrak{f},$$

and consequently

$$\mathfrak{o}_1=\mathfrak{i}''+\mathfrak{f}>\mathfrak{m}+\mathfrak{f}.$$

On the other hand, since $\mathfrak{m}+\mathfrak{f}$ is evidently $>\mathfrak{o}_1$, we have at once

$$(\mathfrak{i}'-\mathfrak{i}'')+\mathfrak{f}=\mathfrak{o}_1.$$

Thirdly, since $\mathfrak{o}_1=\mathfrak{i}'+\mathfrak{f}$ and $\mathfrak{o}_1=\mathfrak{i}''+\mathfrak{f}$, it follows that their product is

$$\mathfrak{o}_1\mathfrak{o}_1=\mathfrak{o}_1=\mathfrak{i}'\mathfrak{i}''+\mathfrak{i}'\mathfrak{f}+\mathfrak{i}''\mathfrak{f}+\mathfrak{f}\mathfrak{f},$$

from which it is seen that

$$\mathfrak{o}_1>\mathfrak{i}'\mathfrak{i}''+\mathfrak{f}.$$

On the other hand, since

$$\mathfrak{i}'\mathfrak{i}''+\mathfrak{f}>\mathfrak{o}_1,$$

it follows that

$$\mathfrak{i}'\mathfrak{i}''+\mathfrak{f}=\mathfrak{o}_1.$$

The product of two ideals $\mathfrak{i}=\mathfrak{i}'\mathfrak{i}''$ *is divisible by them both.* For from $\mathfrak{i}'>\mathfrak{o}_1$, it follows that $\mathfrak{i}'\mathfrak{i}''>\mathfrak{o}_1\mathfrak{i}''$ and that is, $\mathfrak{i}>\mathfrak{i}''$, and similarly $\mathfrak{i}>\mathfrak{i}'$.

ART. **165.** It may be proved further that the laws of division for ideals $\mathfrak{i}$ in $\mathfrak{o}_1$ are the same as those already

found for ideals $\mathfrak{j}$ in $\mathfrak{o}$. This is seen to be true, if we prove the following simple relation which exists between the ideals $\mathfrak{i}$ and $\mathfrak{j}$:

THEOREM. *Corresponding to every ideal* $\mathfrak{i}$ *of* $\mathfrak{o}_1$ *there exists a definite ideal* $\mathfrak{j}$ *of* $\mathfrak{o}$ *which is relatively prime to* $\mathfrak{f}$ *and vice versa, where* $\mathfrak{f}$ *is the ring-leader of the order-modul* $\mathfrak{o}_1$.

1. To prove the first part of this theorem observe, if $\mathfrak{i}$ is an ideal in $\mathfrak{o}_1$, that $\mathfrak{o}\mathfrak{i}$ is an ideal in $\mathfrak{o}$, since it satisfies the required postulate $\mathfrak{o}\mathfrak{o}\mathfrak{i} = \mathfrak{o}\mathfrak{i}$; and from the condition

$$\mathfrak{o}_1 = \mathfrak{i} + \mathfrak{f} \qquad \text{or} \qquad \mathfrak{o}\mathfrak{o}_1 = \mathfrak{o}\mathfrak{i} + \mathfrak{o}\mathfrak{f},$$

it is seen, since $\mathfrak{o}\mathfrak{o}_1 = \mathfrak{o}$, that

$$\mathfrak{o}\mathfrak{i} + \mathfrak{f} = \mathfrak{o},$$

with which is proved the first part of the theorem. Before proceeding to the second part of the theorem it is well to prove two important properties of the realm ideal $\mathfrak{o}\mathfrak{i}$.

If $\mathfrak{i}$ is regarded as the modul

$$\mathfrak{i} = [\tau_1, \tau_2, \cdots, \tau_n],$$

it is seen that

$$\mathfrak{o}\mathfrak{i} > \mathfrak{o}\tau_1 + \mathfrak{o}\tau_2 + \cdots + \mathfrak{o}\tau_n.$$

On the other hand, as each of the products $\mathfrak{o}\tau_k$ is found in $\mathfrak{o}\mathfrak{i}$, it is seen that the realm ideal $\mathfrak{o}\mathfrak{i}$, which corresponds to the ideal $\mathfrak{i}$ of the order-modul, is the greatest common ideal divisor of the basal elements of $\mathfrak{i}$.

It may be proved next that $\mathfrak{i}$ *is the least common multiple of* $\mathfrak{o}\mathfrak{i}$ *and* $\mathfrak{o}_1$, *and that is,*

(I) $$\mathfrak{i} = \mathfrak{o}\mathfrak{i} - \mathfrak{o}_1.$$

For every integer τ which is found in $\mathfrak{o}\mathfrak{i}$ and $\mathfrak{o}_1$ may, due to the relation $\mathfrak{o}_1 = \mathfrak{i} + \mathfrak{f}$, be expressed in the form $\sigma + \varphi$ where σ is an integer of $\mathfrak{i}$ and φ an integer of $\mathfrak{f}$. Since $\varphi = \tau - \sigma$ is an integer of $\mathfrak{o}\mathfrak{i}$, the modul $[1]$ being found in $\mathfrak{o}$, it follows that φ is an integer found in the least common multiple of $\mathfrak{o}\mathfrak{i}$ and $\mathfrak{f}$, and that is, in $\mathfrak{o}\mathfrak{i} - \mathfrak{f}$. With this it is

seen that

$$\mathfrak{o}\mathfrak{i}-\mathfrak{o}_1>\mathfrak{i}+(\mathfrak{o}\mathfrak{i}-\mathfrak{f}). \tag{1}$$

On the other hand, every integer $\sigma+\lambda$, where σ is an integer in $\mathfrak{i}$ and where λ is an integer in both $\mathfrak{o}\mathfrak{i}$ and $\mathfrak{f}$, is an integer in $\mathfrak{o}\mathfrak{i}$ as well as in $\mathfrak{o}_1$. It follows that

$$\mathfrak{i}+(\mathfrak{o}\mathfrak{i}-\mathfrak{f})>\mathfrak{o}\mathfrak{i}-\mathfrak{o}_1. \tag{2}$$

From the relations (1) and (2), we have

$$\mathfrak{i}+(\mathfrak{o}\mathfrak{i}-\mathfrak{f})=\mathfrak{o}\mathfrak{i}-\mathfrak{o}_1. \tag{3}$$

As the product of the least common multiple by the greatest common divisor of two ideals is the product of the two ideals, and that is,

$$(\mathfrak{o}\mathfrak{i}+\mathfrak{f})(\mathfrak{o}\mathfrak{i}-\mathfrak{f})=\mathfrak{o}\mathfrak{i}\cdot\mathfrak{f},$$

we have, since $\mathfrak{o}\mathfrak{i}+\mathfrak{f}=\mathfrak{o}$, the relation

$$\mathfrak{o}\mathfrak{i}-\mathfrak{f}=\mathfrak{i}\cdot\mathfrak{f}.$$

This relation combined with (3) gives

$$\mathfrak{o}\mathfrak{i}-\mathfrak{o}_1=(\mathfrak{o}_1+\mathfrak{f})\mathfrak{i}=\mathfrak{o}_1\mathfrak{i}=\mathfrak{i}.$$

Further, since

$$\mathfrak{o}=\mathfrak{o}\mathfrak{i}+\mathfrak{f}>\mathfrak{o}\mathfrak{i}+\mathfrak{o}_1>\mathfrak{o},$$

it follows that

$$\mathfrak{o}\mathfrak{i}+\mathfrak{o}_1=\mathfrak{o}, \tag{II}$$

and that is, *the greatest common divisor of* $\mathfrak{o}\mathfrak{i}$ *and* $\mathfrak{o}_1$ *is* $\mathfrak{o}$.

2. To prove the second part of the theorem, let $\mathfrak{j}$ be an arbitrary realm ideal that is relatively prime to $\mathfrak{f}$, and that is,

$$\mathfrak{j}+\mathfrak{f}=\mathfrak{o}. \tag{4}$$

Further, let $\mathfrak{i}$ be the least common multiple of $\mathfrak{j}$ and $\mathfrak{o}_1$, or

$$\mathfrak{i}=\mathfrak{j}-\mathfrak{o}_1. \tag{5}$$

To show that $\mathfrak{i}$ is an ideal in $\mathfrak{o}_1$, observe that if τ is an integer which belongs to both the ideal $\mathfrak{j}$ and to the order-modul $\mathfrak{o}_1$, and if $\tilde{\omega}$ is any integer of $\mathfrak{o}_1$, then is $\tilde{\omega}\tau$ found in both $\mathfrak{j}$ and in $\mathfrak{o}_1$ and therefore also in $\mathfrak{i}$.

With this the postulate $\mathfrak{o}_1\mathfrak{i}=\mathfrak{i}$ is seen to be satisfied. Further, due to (4), every integer in $\mathfrak{o}$ and therefore also every integer in $\mathfrak{o}_1$ is of the form $\tilde{\omega}=\tau+\varphi$, where τ is an integer in $\mathfrak{j}$ and φ an integer in $\mathfrak{f}$. From this it follows that $\tau=\tilde{\omega}-\varphi$ is an integer in $\mathfrak{o}_1$. With this it is proved that $\tilde{\omega}=\tau+\varphi$, where τ belongs to both $\mathfrak{j}$ and $\mathfrak{o}_1$, and therefore to $\mathfrak{j}-\mathfrak{o}_1$, and where φ belongs to $\mathfrak{f}$. It follows that

1, $$\mathfrak{o}_1>(\mathfrak{j}-\mathfrak{o}_1)+\mathfrak{f},$$

and of itself it is seen that

2, $$(\mathfrak{j}-\mathfrak{o}_1)+\mathfrak{f}>\mathfrak{o}_1,$$

with the result that

$$\mathfrak{i}+\mathfrak{f}=\mathfrak{o}_1,$$

which is the second of the postulates required that $\mathfrak{i}$ be an ideal in $\mathfrak{o}_1$.

ART. 166. With this it may be proved that the realm ideal $\mathfrak{o}\mathfrak{i}$, which is relatively prime to the realm ideal $\mathfrak{f}$, is identical with the realm ideal $\mathfrak{j}$ above. For, from the relation (5) of the preceding article, it is seen that

(1) $$\mathfrak{o}\mathfrak{i}>\mathfrak{j}.$$

Further, from the equation

$$\mathfrak{i}+\mathfrak{f}=\mathfrak{o}_1, \qquad \text{or} \qquad \mathfrak{o}\mathfrak{i}+\mathfrak{o}\mathfrak{f}=\mathfrak{o}\mathfrak{o}_1,$$

it follows that

$$\mathfrak{o}\mathfrak{i}+\mathfrak{f}=\mathfrak{o},$$

and from this equation, that

(2) $$\mathfrak{o}\mathfrak{i}\mathfrak{j}+\mathfrak{f}\mathfrak{j}=\mathfrak{j}.$$

Observe for realm ideals, we have

$$\mathfrak{f}\mathfrak{j}>\mathfrak{j} \qquad \text{and} \qquad \mathfrak{f}\mathfrak{j}>\mathfrak{f}>\mathfrak{o}_1.$$

Hence, $\mathfrak{f}\mathfrak{j}$ being found in both $\mathfrak{j}$ and $\mathfrak{o}_1$, is found in $\mathfrak{j}-\mathfrak{o}_1$, which from (5) above is $\mathfrak{i}$; and that is,

$$\mathfrak{f}\mathfrak{j}>\mathfrak{i}>\mathfrak{o}\mathfrak{i}, \qquad \text{since} \qquad [1]>\mathfrak{o}.$$

Hence, from (2), it follows that

$$\mathfrak{j} > \mathfrak{o}\mathfrak{i}\mathfrak{j} + \mathfrak{o}\mathfrak{i},$$

or

(3) $$\mathfrak{j} > \mathfrak{o}\mathfrak{i}.$$

And from (1) and (3) we have

$$\mathfrak{o}\mathfrak{i} = \mathfrak{j}.$$

ART. **167.** Through the theorem of the preceding article, it is seen that *there is a correlation between the ideal* $\mathfrak{i}$ *in* $\mathfrak{o}_1$ *and the ideal* $\mathfrak{j}$, *which is relatively prime to* $\mathfrak{f}$ *in* $\mathfrak{o}$, *which correlation is expressed simultaneously through the two relations*

$$\mathfrak{j} = \mathfrak{o}\mathfrak{i} \qquad \text{and} \qquad \mathfrak{i} = \mathfrak{j} - \mathfrak{o}_1.$$

In particular, it is seen that $\mathfrak{o}$ and $\mathfrak{o}_1$ are themselves correlated through these two formulas.

Next observe that

$$\mathfrak{o}\mathfrak{i} + \mathfrak{o}_1 = \mathfrak{o}\mathfrak{i} + \mathfrak{i} + \mathfrak{f} = (\mathfrak{o} + \mathfrak{o}_1)\mathfrak{i} + \mathfrak{f} = \mathfrak{o}\mathfrak{i} + \mathfrak{f} = \mathfrak{o};$$

and on the one hand that

$$(\mathfrak{o}_1, \mathfrak{o}\mathfrak{i}) = (\mathfrak{o}_1, \mathfrak{o}\mathfrak{i} - \mathfrak{o}_1) = (\mathfrak{o}_1, \mathfrak{i}),$$

and on the other that

$$(\mathfrak{o}_1, \mathfrak{o}\mathfrak{i}) = (\mathfrak{o}_1 + \mathfrak{o}\mathfrak{i}, \mathfrak{o}\mathfrak{i}) = (\mathfrak{o}, \mathfrak{o}\mathfrak{i}).$$

It follows that

$$(\mathfrak{o}_1, \mathfrak{i}) = (\mathfrak{o}, \mathfrak{o}\mathfrak{i}) = (\mathfrak{o}, \mathfrak{j}),$$

or

(1) $$N'(\mathfrak{i}) = N(\mathfrak{j}).$$

It is to be noted also that

$$N'(\mathfrak{i}\mathfrak{i}') = N(\mathfrak{o}\mathfrak{i} \cdot \mathfrak{o}\mathfrak{i}') = N(\mathfrak{o}\mathfrak{i})N(\mathfrak{o}\mathfrak{i}') = N'(\mathfrak{i})N'(\mathfrak{i}'),$$

or the norm of the product of two ideals in $\mathfrak{o}_1$ is equal to the product of the norms of these ideals in $\mathfrak{o}_1$.

Finally, it is to be noted if

$$\mathfrak{o}\mathfrak{i}' = \mathfrak{o}\mathfrak{i}'',$$

that $\mathfrak{i}' = \mathfrak{i}''$. This follows at once, when we observe that

$$\mathfrak{i}' = \mathfrak{o}_1 - \mathfrak{o}\mathfrak{i}' \qquad \text{and} \qquad \mathfrak{i}'' = \mathfrak{o}_1 - \mathfrak{o}\mathfrak{i}''.$$

ART. **168. The Primary Theorem.** *If* $\mathfrak{i}$, $\mathfrak{i}'$ *are ideals in* $\mathfrak{o}_1$ *and if* $\mathfrak{i} > \mathfrak{i}'$, *there exists another ideal* $\mathfrak{i}''$ *in* $\mathfrak{o}_1$, *such that* $\mathfrak{i} = \mathfrak{i}'\mathfrak{i}''$.

For if $\mathfrak{i} > \mathfrak{i}'$, then is also

$$\mathfrak{o}\mathfrak{i} > \mathfrak{o}\mathfrak{i}',$$

where $\mathfrak{o}\mathfrak{i}$ and $\mathfrak{o}\mathfrak{i}'$ are realm ideals. It follows (Art. 14) that

$$\mathfrak{o}\mathfrak{i} = \mathfrak{o}\mathfrak{i}'\mathfrak{j}'',$$

where $\mathfrak{j}''$ is a realm ideal. Since $\mathfrak{o}\mathfrak{i}$ is relatively prime to $\mathfrak{f}$, the same is also true of $\mathfrak{j}''$, and from above, it was seen that there is an ideal $\mathfrak{i}''$ in $\mathfrak{o}_1$ such that

$$\mathfrak{o}\mathfrak{i}'' = \mathfrak{j}''.$$

With this it is shown that

$$\mathfrak{o}\mathfrak{i} = \mathfrak{o}\mathfrak{i}' \cdot \mathfrak{o}\mathfrak{i}'' = \mathfrak{o}\mathfrak{i}'\mathfrak{i}'',$$

and from the preceding article, that

$$\mathfrak{i} = \mathfrak{i}'\mathfrak{i}''.$$

That there is only one ideal $\mathfrak{i}''$ in $\mathfrak{o}_1$, which has this property, is seen at once. For, suppose

$$\mathfrak{i} = \mathfrak{i}'\mathfrak{i}'' = \mathfrak{i}'\mathfrak{i}''',$$

where $\mathfrak{i}'''$ is also an ideal in $\mathfrak{o}_1$. It would then follow that

$$\mathfrak{o}\mathfrak{i} = \mathfrak{o}\mathfrak{i}' \cdot \mathfrak{o}\mathfrak{i}'' = \mathfrak{o}\mathfrak{i}' \cdot \mathfrak{o}\mathfrak{i}'''.$$

From the theory of realm ideals it follows that

$$\mathfrak{o}\mathfrak{i}'' = \mathfrak{o}\mathfrak{i}'''$$

and therefore, from above

$$\mathfrak{i}'' = \mathfrak{i}'''.$$

With these results it is established that the laws of divisibility are the same for the ideals in $\mathfrak{o}_1$ as they have been found to be in $\mathfrak{o}$.

ART. **169. Equivalence of Ideals of an Order-Modul.** Two ideals $\mathfrak{i}$ and $\mathfrak{i}'$ of $\mathfrak{o}_1$ are said to be *equivalent*, if there

is a number μ integral or fractional of the fixed realm such that $\mathfrak{i}' = \mu\mathfrak{i}$.

With Bachmann (*Allg. Arith.*, etc., p. 397) we shall require that the norm of μ be *positive*. It is evident that ideals of $\mathfrak{o}_1$ which are all equivalent to one ideal are equivalent to one another. From this it follows that the ideals of $\mathfrak{o}_1$ may be distributed into classes, where the ideals of the same class are equivalent, while two ideals of different classes are not equivalent. That the number of such classes is finite may be proved in a similar way as for example in Art. 84. An independent proof, however, follows.

Observe that the order-modul $\mathfrak{o}_1$ is itself an ideal in $\mathfrak{o}_1$ and accordingly that there exists a class of ideals in $\mathfrak{o}_1$ which are equivalent to $\mathfrak{o}_1$. This class is called the *principal class* and consists by definition of ideals in $\mathfrak{o}_1$ of the form $\tilde{\omega}\mathfrak{o}_1$, where $\tilde{\omega}$ is a number of the fixed realm with positive norm. Since the modul $[1]$ is found in $\mathfrak{o}_1$, it follows from the relation $\tilde{\omega}\mathfrak{o}_1 > \mathfrak{o}_1$, that $\tilde{\omega} > \mathfrak{o}_1$, and that is, $\tilde{\omega}$ is an integer of the order-modul $\mathfrak{o}_1$, and must satisfy the condition

$$\mathfrak{o}_1\tilde{\omega} + \mathfrak{f} = \mathfrak{o}_1.$$

This necessary condition is also sufficient that $\mathfrak{o}_1\tilde{\omega}$ be a principal ideal in $\mathfrak{o}_1$. For, if the integer $\tilde{\omega}$ with positive norm is contained in $\mathfrak{o}_1$, then $\tilde{\omega}\mathfrak{o}_1$ is divisible by $\mathfrak{o}_1$ and $\tilde{\omega}\mathfrak{o}_1$, being an ideal equivalent to $\mathfrak{o}_1$, is a principal ideal in $\mathfrak{o}_1$.

The second form (Art. 14) of the Primary Theorem may be presented here: *If* $\mathfrak{i}$ *is any ideal in* $\mathfrak{o}_1$, *there exists a second ideal* $\mathfrak{i}'$ *in* $\mathfrak{o}_1$ *such that* $\mathfrak{i}\mathfrak{i}'$ *is a principal ideal of* $\mathfrak{o}_1$.

Since by definition $\mathfrak{i}$ and $\mathfrak{f}$ are relatively prime in $\mathfrak{o}_1$, and since 0 and 1 are integers in $\mathfrak{o}_1$, it is always possible to find an integer $\tilde{\omega}$ such that (Vol. I, Art. 143)

$$\tilde{\omega} \equiv 0 \pmod{\mathfrak{i}} \qquad \text{and} \qquad \tilde{\omega} \equiv 1 \pmod{\mathfrak{f}},$$

where (Vol. I, Art. 143, end) $\tilde{\omega}$ may be so chosen that its norm is *positive*.

From the first of these congruences it is seen that

$$\tilde{\omega} > \mathfrak{i} > \mathfrak{o}_1,$$

and accordingly

$$\mathfrak{o}_1\tilde{\omega} > \mathfrak{o}_1,$$

since

$$\mathfrak{o}_1\mathfrak{o}_1 = \mathfrak{o}_1.$$

As $\mathfrak{f} > \mathfrak{o}_1$, it follows also that

$$\tilde{\omega}\mathfrak{o}_1 + \mathfrak{f} > \mathfrak{o}_1. \tag{1}$$

On the other hand from the second of the above congruences, we have

$$1 = \tilde{\omega} + \varphi,$$

where φ is an integer of $\mathfrak{f}$, and therefore also

$$\mathfrak{o}_1 > \mathfrak{o}_1\tilde{\omega} + \mathfrak{o}_1\mathfrak{f} > \mathfrak{o}_1\tilde{\omega} + \mathfrak{f}. \tag{2}$$

From (1) and (2) it is seen that

$$\tilde{\omega}\mathfrak{o}_1 + \mathfrak{f} = \mathfrak{o}_1,$$

which shows that $\tilde{\omega}\mathfrak{o}_1$ *is an ideal in* $\mathfrak{o}_1$.

From the congruence $\tilde{\omega} \equiv 0 \pmod{\mathfrak{i}}$ it follows also that $\tilde{\omega}\mathfrak{o}_1$ is divisible by $\mathfrak{i}$, and hence, from the fundamental theorem above, there exists a second ideal $\mathfrak{i}'$ in $\mathfrak{o}_1$ such that

$$\mathfrak{i}\mathfrak{i}' = \tilde{\omega}\mathfrak{o}_1,$$

which is a principal ideal.

With this it follows also (Art. 82) that *the number of classes of ideals in* $\mathfrak{o}_1$ *is finite.*

It may be proved further that if $\mathfrak{i}'$ belongs to the class C' and $\mathfrak{i}''$ to the class C'', then $\mathfrak{i}'\mathfrak{i}''$ determines a class C. For the product of any two ideals $\mu'\mathfrak{i}'$, $\mu''\mathfrak{i}''$ that are equivalent respectively to $\mathfrak{i}'$ and $\mathfrak{i}''$ is an ideal $\mu'\mu''\mathfrak{i}'\mathfrak{i}''$ which is equivalent to $\mathfrak{i}'\mathfrak{i}''$. We may accordingly write as in Art. 54

$$C'C'' = C.$$

If C_0 is the principal class, then clearly

$$C_0 C = C.$$

Again observe that corresponding to any ideal $\mathfrak{i}$ in $\mathfrak{o}_1$ another ideal $\mathfrak{i}'$ in $\mathfrak{o}_1$ exists, such that $\mathfrak{i}\mathfrak{i}'$ is a principal ideal in $\mathfrak{o}_1$. It follows that if C is any class, there is another class C', such that

$$CC' = C_0.$$

There is only one class C' which satisfies this condition. For, if a second class C'' existed, such that

$$CC'' = C_0,$$

then we would have

$$CC'C'' = C_0 C'' = C_0 C' \qquad \text{or} \qquad C' = C''.$$

Two classes C' and C'' are said to be *reciprocal* or *inverse* (Art. 54) if they satisfy the relation

$$C'C'' = C_0.$$

If A and B are any two classes of $\mathfrak{o}_1$, there is another class C of $\mathfrak{o}_1$, such that

$$A = BC.$$

For the uniquely determined class

$$C = AB',$$

where $BB' = C_0$, satisfies this condition.

ART. **170. The Number of Ideal Classes of an Order-Modul.** The number of ideal classes of an order-modul $\mathfrak{o}_1$ may be determined in the same manner as has already been done for $\mathfrak{o}$ (Arts. 152 ff.).

We must determine first the limiting value

$$\lim_{t \to \infty} \left(\frac{T}{t} \right),$$

where T is the number of principal ideals $\mathfrak{o}_1 \alpha$ in $\mathfrak{o}_1$, whose norms are not greater than t and which are divisible by a given ideal $\mathfrak{i}$ in $\mathfrak{o}_1$. (See Dedekind, *Werke*, Vol. 1, pp. 148 ff.)

These principal ideals $\mathfrak{o}_1\alpha$ are accordingly characterized by the three postulates:

1. α is an integer of $\mathfrak{i}$; and that is, if

$$\mathfrak{i}=[\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n],$$

then is

$$\alpha=a_1\alpha_1+a_2\alpha_2+\cdots+a_n\alpha_n,$$

where the a's are rational integers;

2. $$\mathfrak{o}_1\alpha+\mathfrak{f}=\mathfrak{o}_1;$$

3. $$0<N(\alpha)\leqq t.$$

The first two postulates are expressed through the congruences

$$\alpha\equiv 0 \pmod{\mathfrak{i}}, \qquad \alpha\equiv\tilde{\omega} \pmod{\mathfrak{f}}, \tag{i}$$

where $\tilde{\omega}$ is any of the incongruent (mod. $\mathfrak{f}$) integers of $\mathfrak{o}_1$, for which $\mathfrak{o}_1\tilde{\omega}+\mathfrak{f}=\mathfrak{o}_1$. Denote the number of such integers by $\varphi_1(\mathfrak{f})$. Due to the condition $\mathfrak{i}+\mathfrak{f}=\mathfrak{o}_1$ (Vol. I, 143), the congruences (i) admit solution and their solutions form a definite class of numbers (mod. $\mathfrak{i}-\mathfrak{f}$). Accordingly, there exist $\varphi_1(\mathfrak{f})$ incongruent (mod. $\mathfrak{i}-\mathfrak{f}$) integers α which satisfy the two postulates 1 and 2; and that is, all the integers α which satisfy these two postulates fall into $\varphi_1(\mathfrak{f})$ classes of numbers (mod. $\mathfrak{i}-\mathfrak{f}$).

Next observe, since

$$(\mathfrak{i}-\mathfrak{f})(\mathfrak{i}+\mathfrak{f})=\mathfrak{i}\mathfrak{f}, \qquad \text{and} \qquad \mathfrak{i}+\mathfrak{f}=\mathfrak{o}_1,$$

that

$$(\mathfrak{i}-\mathfrak{f})\mathfrak{o}_1=\mathfrak{i}-\mathfrak{f}=\mathfrak{i}\mathfrak{f}.$$

It follows from the remark found in Art. 109 that

$$\mathfrak{i}k>\mathfrak{i}\mathfrak{f}, \qquad \text{where} \qquad k=(\mathfrak{o},\ \mathfrak{o}_1).$$

It is seen that each representative of the $\varphi_0(\mathfrak{f})$ number-classes (mod. $\mathfrak{i}\mathfrak{f}$) may be distributed into ($\mathfrak{i}\mathfrak{f}$, $\mathfrak{i}k$) number classes (mod. $\mathfrak{i}k$). Hence the number of incongruent (mod. $\mathfrak{i}k$) classes into which the integers α above may be distributed, and that is, the number of classes into which

α may be distributed with respect to the modul

$$[k\alpha_1, k\alpha_2, k\alpha_3, \cdots, k\alpha_n] \qquad \text{(ii)}$$

is

$$c = \varphi_1(\mathfrak{f})(\mathfrak{i}\mathfrak{f}, \mathfrak{i}k). \quad \text{(Note Art. 109, Remark.)}$$

It may be proved that the integer c is independent of the ideal $\mathfrak{i}$ as follows:

Observe that $\mathfrak{i} > \mathfrak{o}_1 > \mathfrak{o}$, and $\mathfrak{i} > \mathfrak{o}\mathfrak{i} > \mathfrak{o}$. It follows that

$$(\mathfrak{o}, \mathfrak{i}) = (\mathfrak{o}, \mathfrak{o}_1)(\mathfrak{o}_1, \mathfrak{i}),$$

and also

$$(\mathfrak{o}, \mathfrak{i}) = (\mathfrak{o}, \mathfrak{o}\mathfrak{i})(\mathfrak{o}\mathfrak{i}, \mathfrak{i}),$$

so that

$$(\mathfrak{o}, \mathfrak{o}_1)(\mathfrak{o}_1, \mathfrak{i}) = (\mathfrak{o}, \mathfrak{o}\mathfrak{i})(\mathfrak{o}\mathfrak{i}, \mathfrak{i}).$$

Since

$$N'(\mathfrak{i}) = (\mathfrak{o}_1, \mathfrak{i}) = N(\mathfrak{o}\mathfrak{i}) = (\mathfrak{o}, \mathfrak{o}\mathfrak{i}),$$

it follows from the relation just written that

$$\text{(a)} \qquad k = (\mathfrak{o}\mathfrak{i}, \mathfrak{i}) = (k\mathfrak{o}\mathfrak{i}, k\mathfrak{i}).$$

Further, since

$$k\mathfrak{o}\mathfrak{i} > \mathfrak{f}\mathfrak{o}\mathfrak{i} = \mathfrak{f}\mathfrak{i} > \mathfrak{o},$$

we have

$$(\mathfrak{o}, k\mathfrak{o}\mathfrak{i}) = (\mathfrak{o}, \mathfrak{f}\mathfrak{i})(\mathfrak{f}\mathfrak{i}, \mathfrak{o}k\mathfrak{i}),$$

or

$$\text{(b)} \qquad (\mathfrak{f}\mathfrak{i}, \mathfrak{o}k\mathfrak{i}) = \frac{N(\mathfrak{o}k\mathfrak{i})}{N(\mathfrak{f}\mathfrak{i})} = \frac{N(\mathfrak{o}k)}{N(\mathfrak{f})} = \frac{k^n}{N(\mathfrak{f})}.$$

And, using the formula (a), it is seen that

$$(\mathfrak{f}\mathfrak{i}, k\mathfrak{i}) = (\mathfrak{f}\mathfrak{i}, \mathfrak{o}k\mathfrak{i})(\mathfrak{o}k\mathfrak{i}, k\mathfrak{i}) = \frac{k^{n+1}}{N(\mathfrak{f})},$$

with the result that

$$c = \frac{\varphi_0(\mathfrak{f})}{N(\mathfrak{f})} k^{n+1}$$

is a definite value which depends *only* upon $\mathfrak{o}_1$.

ART. **171.** If out of each of the c classes of numbers (mod. $k\mathfrak{i}$) of the preceding article, an integer

$$g_1^{(\nu)}\alpha_1 + g_2^{(\nu)}\alpha_2 + \cdots + g_n^{(\nu)}\alpha_n \qquad (\nu = 1, 2, \cdots, c)$$

is taken, it is seen that all the integers α, which satisfy the

postulates 1 and 2 (note formula (ii)), are had through the expressions (see (ii), Art. 170)

$$(1)\quad \alpha=(g_1^{(\nu)}+ka_1)\alpha_1+(g_2^{(\nu)}+ka_2)\alpha_2+\cdots+(g_n^{(\nu)}+ka_n)\alpha_n \qquad (\nu=1, 2, \cdots, c),$$

where the quantities a_i run through all rational integers. It is seen that in this formula each α is had only once.

Postulate 3 requires that in addition each α satisfy the condition

$$(2)\qquad 0<N(\alpha)\leqq t,$$

where $N(\alpha)$ must be taken positive in every case.

Observe next that if α satisfies the three postulates and if ϵ is a unit in $\mathfrak{o}_1$ with positive norm, that the associate integer $\epsilon^m\alpha$, where m is any rational integer, also satisfies the three postulates.

Proceeding as in Art. 127, let $\epsilon_1, \epsilon_2, \cdots, \epsilon_{s-1}$ be a system of fundamental units in $\mathfrak{o}_1$, with positive norm, and of the associated integers $\epsilon\alpha$, determine those whose exponents (Art. 151) $e_i(\alpha)$ in the equations

$$l_i(\alpha)=e_1(\alpha)l_{i1}+e_2(\alpha)l_{i2}+\cdots+e_{s-1}(\alpha)l_{i,\,s-1}+fc_i \qquad (i=1, 2, \cdots, s)$$

satisfy the inequalities

$$(3)\qquad 0\leqq e_i(\alpha)<1 \qquad (i=1, 2, \cdots, s-1).$$

It is observed that the number of α's thus isolated is the same as the number of reduced units in $\mathfrak{o}_1$ and that is, the number of roots of unity in $\mathfrak{o}_1$. If this number is denoted by ρ_0, it follows that the number of α's which are determined through the formulas (1), (2), and (3) is $\rho_0 T$.

The limiting value of $\frac{T}{t}$ may be determined as in Arts. 152 ff. Observe, however, that in Art. 170 the α's are limited to the one linear form, whereas here there are c linear forms as put forth in formula (1) above. For each

of these we may write as in Art. 152

$$u_1 = \delta g_1^{(\nu)} + \delta k a_1,\ u_2 = \delta g_2^{(\nu)} + \delta k a_2,\ \cdots,\ u_n = \delta g_n^{(\nu)} + \delta k a_n.$$

Note that when t becomes indefinitely large, $\delta = \frac{1}{t^n}$ becomes indefinitely small, with the result that the above formulae become

$$u_1 = k\delta a_1,\ u_2 = k\delta a_2,\ \cdots,\ u_n = k\delta a_n.$$

Accordingly, the formula at end of Art. 152 becomes

$$\int \cdots \int du_1 du_2 \cdots du_n = \rho_0 k^n \lim_{t\to\infty} \left(\frac{T}{t}\right). \tag{4}$$

Note that the discriminant $\Delta(\alpha_1, \alpha_2, \cdots, \alpha_n)$ of the ideal $\mathfrak{i}$ is equal to $N'(\mathfrak{i})^2 D_1$, where D_1 is the discriminant of the order-modul $\mathfrak{o}_1$. The value of the above integral is for each of the forms (1), see Art. 153

$$\frac{2^{s-\sigma}\pi^{n-s}\,|l_k(\epsilon_i)|}{N'(\mathfrak{i})\,|\sqrt{D_1}|}.$$

Since

$$D_1 = N(\mathfrak{o}_1)^2 D = k^2 D,$$

we have from formula (4), when taken over the c linear forms (1), the value

$$\lim_{t\to\infty} \left(\frac{T}{t}\right) = \frac{\varphi_1(\mathfrak{f})}{N(\mathfrak{f})} \cdot \frac{2^{s-\sigma}\pi^{n-s}}{N'(\mathfrak{i})\,|\sqrt{D}|}\, Q_1,$$

where for brevity

$$Q_1 = \frac{|l_k(\epsilon_i)|}{\rho_0}$$

denotes the ratio of the regulator of the system of fundamental units of $\mathfrak{o}_1$ to the number of the roots of unity of this order-modul.[1]

ART. **172.** Denote by $F(k)$ the number of principal ideals in $\mathfrak{o}_1$, which are divisible by $\mathfrak{i}$, and whose norms are

[1] See Bachmann, p. 404.

equal to k. It follows as in Art. 157 that

$$\underset{t\to\infty}{L}\left(\frac{T}{t}\right)=\underset{\nu\to\infty}{L}\frac{F(1)+F(2)+\cdots+F(\nu)}{\nu},$$

and that

$$\underset{t\to\infty}{L}\left(\frac{T}{t}\right)=\underset{\lambda\to 1}{L}(\lambda-1)\sum\frac{1}{N'(\mathfrak{o}_1\alpha)^\lambda},$$

where the summation is to be taken over all the principal ideals in $\mathfrak{o}_1$, which are divisible by $\mathfrak{i}$. It follows from the formula of the preceding article that

$$\underset{\lambda\to 1}{L}(\lambda-1)\sum\frac{1}{N'(\mathfrak{o}_1\alpha)^\lambda}=\frac{\varphi_1(\mathfrak{f})}{N(\mathfrak{f})}\frac{2^{s-\sigma}\pi^{n-s}Q_1}{N'(\mathfrak{i})\,|\sqrt{D}|}.$$

If $\mathfrak{a}$ goes over all the ideals of a given class C in $\mathfrak{o}_1$, and if $\mathfrak{i}$ is a definite ideal of the reciprocal class C', then every product $\mathfrak{a}\mathfrak{i}$ is an ideal in $\mathfrak{o}_1$ which belongs to the principal class $C_0=CC'$; and that is, $\mathfrak{a}\mathfrak{i}=\mathfrak{o}_1\alpha$, say. If, on the other hand, $\mathfrak{o}_1\alpha$ is a principal ideal that is divisible by $\mathfrak{i}$, there exists a definite ideal $\mathfrak{a}$ in $\mathfrak{o}_1$ such that $\mathfrak{o}_1\alpha=\mathfrak{i}\mathfrak{a}$, where $\mathfrak{a}$ belongs to the class C, which is the class reciprocal to the class C', in which is found the ideal $\mathfrak{i}$.

Further, since

$$N'(\mathfrak{a}\mathfrak{i})=N'(\mathfrak{a})N'(\mathfrak{i}),$$

it is seen that the summation taken over all the principal ideals in $\mathfrak{o}_1$, that are divisible by $\mathfrak{i}$, is

$$\sum\frac{1}{N'(\mathfrak{o}_1\alpha)^\lambda}=\frac{1}{N'(\mathfrak{i})^\lambda}\sum\frac{1}{N'(\mathfrak{a})^\lambda},$$

where the summation on the right goes over all the ideals of the class C.

Accordingly the formula written above becomes

$$\underset{\lambda\to 1}{L}(\lambda-1)\sum\frac{1}{N'(\mathfrak{a})^\lambda}=\frac{\varphi_1(\mathfrak{f})}{N(\mathfrak{f})}\frac{2^{s-\sigma}\pi^{n-s}}{|\sqrt{D}|}Q_1.$$

The expression on the right being a constant, it follows

from this formula that *the summation on the left has the same value for every class of equivalent ideals in* $\mathfrak{o}_1$.

ART. **173.** Next write

$$Z_0(\lambda) = \sum \frac{1}{N'(\mathfrak{i})^\lambda},$$

where $\lambda > 1$ and where the summation is taken over all the ideals $\mathfrak{i}$ of $\mathfrak{o}_1$. Also put

$$Z(\lambda) = \sum \frac{1}{N(\mathfrak{j})^\lambda} = \prod_{\mathfrak{p}} \left(\frac{1}{1 - \frac{1}{N(\mathfrak{p})^\lambda}} \right),$$

where $\mathfrak{j}$ goes over all the ideals of $\mathfrak{o}$.

If $\mathfrak{p}'$ denotes the prime ideal factors of $\mathfrak{f}$, and $\mathfrak{p}''$ all other prime ideals in $\mathfrak{o}$, it is seen that

$$Z(\lambda) = \prod_{\mathfrak{p}'} \left(\frac{1}{1 - \frac{1}{N(\mathfrak{p}')^\lambda}} \right) \prod_{\mathfrak{p}''} \left(\frac{1}{1 - \frac{1}{N(\mathfrak{p}'')^\lambda}} \right),$$

or

$$Z(\lambda) = \prod_{\mathfrak{p}'} \left(\frac{1}{1 - \frac{1}{N(\mathfrak{p}')^\lambda}} \right) \Sigma' \frac{1}{N(\mathfrak{j})^\lambda},$$

where the last summation is to be taken over the ideals $\mathfrak{j}$ in $\mathfrak{o}$, that are relatively prime to $\mathfrak{f}$. Since there is always an ideal $\mathfrak{i}$ in $\mathfrak{o}_1$ that corresponds to the ideal $\mathfrak{j}$ in such a way that $\mathfrak{j} = \mathfrak{i}\mathfrak{o}$, and $N(\mathfrak{j}) = N'(\mathfrak{i})$, the summation $\Sigma' \frac{1}{N(\mathfrak{j})^\lambda}$ is nothing other than Z_0.

Further, observing that (Art. 34)

$$\varphi(\mathfrak{f}) = N(\mathfrak{f}) \prod_{\mathfrak{p}'} \left(1 - \frac{1}{N(\mathfrak{p}')} \right),$$

it is seen that

$$\frac{\varphi(\mathfrak{f})}{N(\mathfrak{f})} \lim_{\lambda \to 1} (\lambda - 1) Z(\lambda) = \lim_{\lambda \to 1} (\lambda - 1) Z_0(\lambda).$$

Next, see Formula (5) of Art. 157, it follows from the

above formula that

$$\frac{\varphi(\mathfrak{f})}{N(\mathfrak{f})}\frac{2^{\nu-\sigma}\pi^{n-s}Q}{|\sqrt{D}|}h=\lim_{\lambda\to 1}(x-1)Z_0(\lambda).$$

Note that the left hand side of this expression is constant and that the limit

$$\lim_{\lambda\to 1}(\lambda-1)Z_0(\lambda)$$

is a sum of individual parts, each corresponding to a class of equivalent ideals in $\mathfrak{o}_1$. It follows from the formula at the end of the preceding article that each part has the same value. Further, the number of these parts, and that is, of the number of ideal classes in $\mathfrak{o}_1$ is finite, which number from the formula above is determined through the relation

$$\frac{\varphi(\mathfrak{f})}{N(\mathfrak{f})}\frac{2^{s-\sigma}\pi^{n-s}Q}{|\sqrt{D}|}h=\frac{\varphi_1(\mathfrak{f})}{N(\mathfrak{f})}\frac{2^{s-\sigma}\pi^{n-\sigma}Q_1}{|\sqrt{D}|}h_1,$$

or

$$\frac{h}{h_1}=\frac{\varphi_1(\mathfrak{f})}{\varphi(\mathfrak{f})}\frac{Q_1}{Q}.$$

With this[1] *the ratio of the number of classes of equivalent ideals in* $\mathfrak{o}$ *to the number of classes of equivalent ideals in* $\mathfrak{o}_1$ *is determined, as is also the ratio of the numbers of classes of equivalent ideals in* $\mathfrak{o}_1$ *and* $\mathfrak{o}_2$, *where* $\mathfrak{o}_2$ *is any other oder-modul.*

[1] Dedekind, *Werke*, Vol. I, pp. 137 ff.; see also H. Weber, *Math. Ann.*, Vol. 48, pp. 433 ff.; and Artin, *Math. Ann.*, Vol. 89, pp. 147–156.

CHAPTER XI

COMPOSITE (FACTORABLE) FORMS

ART. **174.** In Chapter XII of Vol. I was developed a correlation between the ideals of a quadratic realm and the theory of quadratic forms. In an analogous manner there exists a correlation between the ideals of realms of the nth degree and certain forms which we shall call *composite* [1] (factorable) forms of the nth degree in n variables. This theory as developed by Dedekind [2] will be treated here. By a form of the nth degree in n variables (indeterminates) $u_1, u_2, \cdots, u_n$ is to be understood an integral, homogeneous function of the nth dimension in these indeterminates. Such a form is said to be *composite* if it may be expressed as a product of n linear forms.

Let such a form be

$$F(u_1, u_2, \cdots, u_n) = U_1 \cdot U_2 \cdots U_n, \tag{1}$$

where

$$U_i = \omega_{i1}u_1 + \omega_{i2}u_2 + \cdots + \omega_{in}u_n \quad (i = 1, 2, \cdots, n), \tag{2}$$

the quantities ω_{ik} being any algebraic numbers. The functional determinant (Jacobian) of the U's with respect to the u's, and that is

$$J\frac{(U_1, U_2, \cdots, U_n)}{(u_1, u_2, \cdots, u_n)},$$

is the determinant of the equations (2), whose square

[1] These forms were first treated by Lagrange: "Sur la solution des problèmes indétermines du second degré," *Mem. de l'Ac. de Berlin*, Vol. 23, 1769, § VI; *Works of Lagrange* (1868), Vol. II, p. 375. They were called *zerlegbar* by Kronecker.

[2] Dedekind, *Zahlentheorie*, § 182, 4th Edition. See also Bachmann, *Allgemeine Arth. der Zahlkörper*, Chapter X.

shall be *defined* as the discriminant [1] of the form F and denoted by

$$\Delta(F) = |\omega_{ik}|^2. \tag{3}$$

Observe that the decomposition of the form F into linear factors is *not* unique since

$$F(u_1, u_2, \cdots, u_n) = c_1 U_1 \cdot c_2 U_2 \cdots c_n U_n,$$

where

$$c_1 \cdot c_2 \cdots c_n = 1.$$

And note that the discriminant of the form is definitely determined.

From (1) and (2) it follows that

$$\frac{\partial \log F}{\partial u_r} = \sum_{i=r}^{i=n} \frac{\omega_{ir}}{U_i}, \qquad \frac{\partial^2 \log F}{\partial u_r \partial u_s} = -\sum_{i=r}^{i=n} \frac{\omega_{ir} \cdot \omega_{is}}{U_i^2},$$

and consequently the determinant

$$\left| \frac{\partial^2 \log F}{\partial u_r \partial u_s} \right| = (-1)^n \frac{\Delta(F)}{F^2}. \tag{4}$$

On the other hand, it is seen that

$$\frac{\partial^2 \log F}{\partial u_r \partial u_s} = \frac{1}{F^2}\left(F \frac{\partial^2 F}{\partial u_r \partial u_s} - \frac{\partial F}{\partial u_r} \cdot \frac{\partial F}{\partial u_s}\right).$$

Form the determinant

$$D(F) = \begin{vmatrix} F, & \frac{\partial F}{\partial u_1}, & \frac{\partial F}{\partial u_2}, & \cdots, & \frac{\partial F}{\partial u_n} \\ \frac{\partial F}{\partial u_1}, & \frac{\partial^2 F}{\partial u_1 \partial u_1}, & \frac{\partial^2 F}{\partial u_1 \partial u_2}, & \cdots, & \frac{\partial^2 F}{\partial u_1 \partial u_n} \\ \cdots, & \cdots, & \cdots, & \cdots, & \cdots \\ \cdots, & \cdots, & \cdots, & \cdots, & \cdots \\ \frac{\partial F}{\partial u_n}, & \frac{\partial^2 F}{\partial u_n \partial u_1}, & \frac{\partial^2 F}{\partial u_n \partial u_2}, & \cdots, & \frac{\partial^2 F}{\partial u_n \partial u_n} \end{vmatrix}. \tag{5}$$

Multiply the last n rows of this determinant by F. Then multiply the first row respectively by

$$\frac{\partial F}{\partial u_1}, \frac{\partial F}{\partial u_2}, \cdots, \frac{\partial F}{\partial u_n}.$$

[1] See Hermite, *Crelle's Journal*, Vol. 47, p. 331.

Subtract each of the latter expressions from each of the former with the result that all the terms of the first column vanish except the first. It follows that

$$F^n D(F) = F^{2n+1} \left| \frac{\partial^2 \log F}{\partial u_r \partial u_s} \right|,$$

or

$$D(F) = F^{n+1} \left| \frac{\partial^2 \log F}{\partial u_r \partial u_s} \right|. \tag{6}$$

Making use of (4), it is seen that

$$D(F) = (-1)^n F^{n-1} \Delta(F). \tag{7}$$

If the function F has integral coefficients and if t is the greatest common divisor of these coefficients, it follows from (6) that $D(F)$ has t^{n+1} as a divisor and from (7) that $\Delta(F)$ is divisible by t^2.

It is further seen from the definition of the discriminant of the form, if k is any constant, that the equation

$$\Delta(kF) = k^2 \Delta(F) \tag{8}$$

exists, whether the coefficients in F are integral or fractional.

ART. **175.** We shall next specialize the theory by treating *composite* forms of a fixed realm of rationality Ω, say, of the nth degree. Such a form is $F(u_1, u_2, \cdots, u_n)$, if it may be expressed as the norm of a linear form [1]

$$\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n, \tag{1}$$

where α_i are numbers (fractional or integral) of Ω. The coefficients of $F(u_1, u_2, \cdots, u_n)$ are rational numbers.

Certain limitations are to be observed: *First*, the coefficients α_i cannot all belong to a realm Ω' of degree n', where $n = n' \cdot m$ and m is a positive integer. For in this

[1] See Part II of Kronecker's *Grundzüge*, in particular § 14, end, and § 19, end. Kronecker indicates somewhat vaguely his theory of *divisors* "through which with the help of linear forms is effected a transition from complex numbers to composite forms." See also Kummer, *Crelle*, 35, p. 342, and again Kronecker. *Grundzüge*, §§ 22, 23, 24, 25.

case the norm with respect to Ω' of the linear form (1) is a form $F_1(u_1, u_2, \cdots, u_n)$, where the coefficients are rational numbers, and $F = F_1^m$. Accordingly we must assume that F is an irreducible function in the stock-realm.

In the *second* place, there must not be among the α's any relation such as

$$\alpha_n = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_{n-1}\alpha_{n-1},$$

where the c's are rational numbers. For in this case (1) becomes

$$\alpha_1(u_1 + c_1u_n) + \alpha_2(u_2 + c_2u_n) + \cdots + \alpha_{n-1}(u_{n-1} + c_{n-1}u_n),$$

so that the original n indeterminates are now replaced by the $n-1$ indeterminates

$$u_1 + c_1u_n,\ u_2 + c_2u_n,\ \cdots,\ u_{n-1} + c_{n-1}u_n.$$

Hence, if it is assumed that the n indeterminates u are independent, the coefficients $\alpha_1, \alpha_2, \cdots, \alpha_n$ must be rationally independent, and that is, they cannot belong to a realm of degree less than n.

Accordingly, *a composite form of the nth degree of a fixed realm is defined as an irreducible form of the nth degree in n independent indeterminates* u_i. *And this form may be expressed as the norm of a linear form (1) whose coefficients* α_i *belong to a definite realm of rationality.*

It follows that *the coefficients* $\alpha_1, \alpha_2, \cdots, \alpha_n$ *form a basis of this realm. The form F is said to be primitive or a unit form, if its coefficients are rational integers whose greatest common divisor is unity.* (Art. 67.)

ART. **176. The Relation of the Discriminant of a Composite Form of the Realm to the Fundamental Invariant.** Let $E(u_1, u_2, \cdots, u_n)$ be a composite unit form of the realm of the nth degree with the n indeterminates $u_1, u_2, \cdots, u_n$. Let U_1 be one of its linear factors. The coefficients of U_1 as seen above form a basis of the realm, but as seen in Art. 174, they are not

necessarily integers of the realm. However, it is always possible to choose an integer γ of the realm such that

$$\gamma U_1 = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n, \tag{1}$$

where the α's are algebraic integers. This linear form may be denoted by

$$f = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n. \tag{2}$$

If the indeterminates u are allowed to take only rational integral values, it is seen that f is identical with the modul

$$\mathfrak{m} = [\alpha_1, \alpha_2, \cdots, \alpha_n].$$

The quotient $\frac{\mathfrak{m}}{\mathfrak{m}}$ is an order-modul $\mathfrak{o}_1$, say; and $\mathfrak{o}_1\mathfrak{m} > \mathfrak{m}$. If

$$\mathfrak{o}_1 = [\tilde{\omega}_1, \tilde{\omega}_2, \cdots, \tilde{\omega}_n],$$

it follows that $\tilde{\omega}_i \alpha_k$ are numbers of $\mathfrak{m}$, and may therefore be expressed as linear functions of the α's with rational integral coefficients. Accordingly, we may write

$$f\tilde{\omega}_i = U_{i1}\alpha_1 + U_{i2}\alpha_2 + \cdots + U_{in}\alpha_n \quad (i = 1, 2, \cdots, n),$$

where the quantities U_{ik} are linear homogeneous functions of the u's with rational integral coefficients.

The determinant

$$U = |U_{ik}| \tag{3}$$

of the n equations above is a homogeneous integral function of the nth degree in the u's whose coefficients are rational integers.

Since the integers $\tilde{\omega}_1, \tilde{\omega}_2, \cdots, \tilde{\omega}_n$ form a basis (not necessarily of all integers) of $\mathfrak{o}$, it is seen that

$$\alpha_i = r_{i1}\tilde{\omega}_1 + r_{i2}\tilde{\omega}_2 + \cdots + r_{in}\tilde{\omega}_n \quad (i = 1, 2, \cdots, n), \tag{4}$$

whose determinant in absolute value (see Art. 11) is

$$|r_{ik}| = \frac{(\mathfrak{o}, \mathfrak{m})}{(\mathfrak{m}, \mathfrak{o})}. \tag{5}$$

If the values of α_i from (4) are written in (2), it is seen

that

$$f\tilde{\omega}_i = \sum_{k,h} U_{ik} r_{kh} \tilde{\omega}_h \qquad (i=1, 2, \cdots, n). \tag{6}$$

From this formula it follows (Art. 70) that

$$N(f) = |r_{ik}|\, U, \tag{7}$$

where for the u's that appear in f and U may be written any rational integers.

The function U defined through formulas (3) and (7) is accordingly a composite form that corresponds to or is associated with the modul $\mathfrak{m}$.

Suppose that instead of the modul $\mathfrak{m} = [\alpha_1, \alpha_2, \cdots, \alpha_n]$, the form f is considered with respect to the ideal

$$\mathfrak{i} = (\alpha_1, \alpha_2, \cdots, \alpha_n). \tag{8}$$

By definition (Art. 68) $\mathfrak{i}$ is the content of the linear form f. From (2) it is seen, if E denotes a unit form, that

$$EN(\gamma) = N(f);$$

and, as

$$N(f) = EN(\mathfrak{i}), \tag{9}$$

we have

$$N(\mathfrak{i}) = N(\gamma).$$

The integers α_i need not be the basis of the ideal $\mathfrak{i}$ in (8). If $\beta_1, \beta_2, \cdots, \beta_n$ form such a basis, it is seen that

$$\alpha_i = a_{i1}\beta_1 + a_{i2}\beta_2 + \cdots + a_{in}\beta_n \qquad (i=1, 2, \cdots, n), \tag{10}$$

where the a's are rational integers. Further, since the β's are integers in $\mathfrak{o} = [\omega_1, \omega_2, \cdots, \omega_n]$, it follows that

$$\beta_i = b_{i1}\omega_1 + b_{i2}\omega_2 + \cdots + b_{in}\omega_n \qquad (i=1, 2, \cdots, n). \tag{11}$$

Accordingly, it follows that

$$\alpha_i = c_{i1}\omega_1 + c_{i2}\omega_2 + \cdots + c_{in}\omega_n \qquad (i=1, 2, \cdots, n),$$

where the determinant

$$|c_{ik}| = |a_{ik}|\,|b_{ik}|$$

is different from zero.

From the definition of the discriminant of a form in Art. 174, it is seen that

$$\Delta[N(f)] = |a_{ik}|^2 \cdot |b_{ik}|^2 D, \tag{12}$$

where D is the fundamental invariant of the fixed realm.

It follows from (11) that

$$|b_{ik}| = N(\mathfrak{i}).$$

From formula (9) we have, on the other hand

$$\Delta[N(f)] = N(\mathfrak{i})^2 \Delta(E). \tag{13}$$

From (11), (12), and (13) we have

$$\Delta(E) = |a_{ik}|^2 D. \tag{14}$$

It is thus seen that *the fundamental invariant D, to which a composite unit form belongs, is always a divisor of the discriminant of this form, the ratio of the latter to the former being the square of a rational integer.*

It is clear that for a given value $\Delta(E)$ the integer D can have only a finite number of different values; and, since for a given D there exist (Art. 136) only a finite number of realms of the nth degree, it follows that the number of composite unit forms of the nth degree with given discriminant may be distributed into only a finite number of realms of the nth degree. Reciprocally, the discriminants of all composite unit-forms, which belong to a definite realm, are quadratic multiples of its fundamental invariant. It is also evident that the necessary and sufficient condition that the discriminant of the unit-form be equivalent to the fundamental invariant is that

$$|a_{ik}| = \pm 1,$$

and that is, that the α's [cf. formulas (10) and (11)] form a basis of the ideal $\mathfrak{i}$.

With this is proved the theorem that *every composite unit-form, which belongs to a definite realm of the nth degree and whose discriminant is equal to the fundamental*

invariant, corresponds to an ideal of the realm

$$\mathfrak{i} = [\alpha_1, \alpha_2, \cdots, \alpha_n],$$

whose linear form is f, and which may be determined through the form E in the manner indicated above.

ART. **177.** We may next prove the inverse of the theorem just stated, namely: *Corresponding to every ideal* $\mathfrak{i}$ *of the fixed realm there exists a unit-form U, whose discriminant is equal to the fundamental invariant D.*

For, let the modul $\mathfrak{m} = [\alpha_1, \alpha_2, \cdots, \alpha_n]$ be an ideal and observe (Art. 4) that the order-modul $\mathfrak{o}_1$ of $\mathfrak{m}$ is $\mathfrak{o}$ and that the basal elements of $\mathfrak{o}_1$ are those of $\mathfrak{o}$. Accordingly, it follows that the rational numbers of (4), Art. 176, are in the present case integers, and that

$$|r_{ik}| = (\mathfrak{o}, \mathfrak{m}) = N(\mathfrak{m}).$$

Accordingly, the relation (7) of Art. 176 becomes here

$$N(f) = N(\mathfrak{m})U. \tag{1}$$

We have next to show that U is a unit-form. Suppose that the u's are replaced by any rational integers and that accordingly f becomes an integer α of the ideal $\mathfrak{m} = [\alpha_1, \alpha_2, \cdots, \alpha_n]$. Since α is divisible by $\mathfrak{m}$, it follows that

$$\mathfrak{o}\alpha = \mathfrak{m} \cdot \mathfrak{n}, \tag{2}$$

where $\mathfrak{n}$ is another ideal of the fixed realm. Further (Art. 66, Example 1), the ideal $\mathfrak{n}$ may be so chosen that it is relatively prime to any given ideal, say $\mathfrak{o}g$, where g is a rational integer.

It follows from (2) that

$$\pm N(\alpha) = N(\mathfrak{m})N(\mathfrak{n}),$$

and therefore, from (1) that

$$U = \pm N(\mathfrak{n}). \tag{3}$$

With this it is seen that by a choice of the u's, $N(\mathfrak{n})$ and therefore U may be made relatively prime to any rational integer. Accordingly, the greatest common

divisor of the coefficients of U must be unity, and that is, U is a unit form.

From (1) it follows that

$$\Delta[N(f)]=N(\mathfrak{m})^2\Delta U,$$

and from (13) and (14) of the preceding article

$$\Delta U=D.$$

With this it is proved that U is a unit-form with discriminant equal to the fundamental invariant D and it is seen that U is completely determined through the ideal $(\alpha_1, \alpha_2, \cdots, \alpha_n)=\mathfrak{m}$.

ART. **178.** The values which the form U takes when the indeterminates u are given rational integral values, are called the *numbers* (*integers*) *expressible through the form* U.

To determine more precisely what these numbers are, it may be observed that when a system of integral rational values is given to the u's, the linear form f becomes an integer α of the ideal $\mathfrak{m}$ and accordingly $\mathfrak{o}\alpha=\mathfrak{m}\cdot\mathfrak{n}$, as above.

Thus, corresponding to a definite system of rational integers there exists an ideal $\mathfrak{n}$, and the unit-form U takes the values $+N(\mathfrak{n})$ or $-N(\mathfrak{n})$ according as the norm of α is positive or negative. (See formula (1) of the preceding article.)

Suppose first that $N(\alpha)$ has a *positive* value. Then the ideals $\mathfrak{n}$ include all the ideals of the class C', where C' is the reciprocal class of the class C to which $\mathfrak{m}$ belongs. And that is,

$$CC'=C_0,$$

C_0 being the principal class.

Observe here that $\mathfrak{m}\mathfrak{n}=\mathfrak{o}\alpha$, where $N(\alpha)$ is positive. The norms of all ideal of the class C' are positive integers which may be expressed through the form U. If in the

ideal $\mathfrak{m}$ there exist no integers α with negative norms, then the norms indicated above are the only ones that can be expressed through U.

If, however, integers α of $\mathfrak{m}$ exist with negative norms, there are other ideals $\mathfrak{n}$ (where $\mathfrak{o}\alpha = \mathfrak{m}\cdot\mathfrak{n}$) which form a class C''. This class is in general different from the class C'. The class C' may be said to be *half-equivalent* to C'' and the values of the indeterminates u_i that correspond to α are such that $-N(\mathfrak{n}) = U$. In this case all positive integers that may be expressed through U are the norms of the ideals of the class C', while all negative integers that may be expressed through U are the norms of the ideals of the class C'' with negative sign.

In particular, if there exist units of the realm with negative norm, then since

$$\mathfrak{o}(\epsilon\alpha) = \mathfrak{o}(\alpha) = \mathfrak{m}\mathfrak{n},$$

it follows that the values of u_i which correspond to the number $\epsilon\alpha$ offer a number which may be expressed through the negative norm of $\mathfrak{n}$. In this particular case, the numbers that may be expressed through U are the positive and negatively taken norms of all the ideals of the class C'.

If $\pm g$ is any integer that may be expressed through U, then from above, g must be the norm of an ideal that belongs either to the class C' or C''. There are, however, an infinite number of equivalent ideals that belong to one or the other of these two classes, whose norms are equal to g, and accordingly, there are an indefinite number of ways of expressing $\pm g$ through the form U. These ways, and that is, the different systems of the u's may be united in a group. For, if

$$\mathfrak{n}' = \epsilon\mathfrak{n} \qquad \text{and} \qquad \mathfrak{m}\mathfrak{n} = \mathfrak{o}\alpha,$$

then also is

$$\mathfrak{m}\mathfrak{n}' = \mathfrak{o}(\epsilon\alpha),$$

where ϵ is a unit. There corresponds to every such unit at the same time with the number $\epsilon\alpha$ of $\mathfrak{m}$ a system of values of the u's through which the integer $\pm g$ may be expressed in the form

$$\pm g = \pm N(\mathfrak{n}) = \pm N(\mathfrak{n}'),$$

where the sign is the sign of $N(\alpha)$ and where the norm of ϵ is $+1$.

Corresponding to this expression of integers through the unit form U by ascribing integral values to the systems of indeterminates u_i, there exists the complete analogy with the theorems of Chap. XII of Volume I, through which theorems the expression of numbers through binary quadratic forms were distributed into groups which belong to certain definite roots of congruences. (See Vol. I, Art. 280.)

ART. **179.** This analogy between the more general and the indicated more particular forms may be carried much further. For, let the basis $\alpha_1, \alpha_2, \cdots, \alpha_n$ of $\mathfrak{m}$ be replaced by any other basis $\beta_1, \beta_2, \cdots, \beta_n$, where

$$\beta_i = a_{i1}\alpha_1 + a_{12}\alpha_2 + \cdots + a_{in}\alpha_n \quad (i=1, 2, \cdots, n),$$

the a's being rational integers so chosen that

$$|a_{ik}| = +1.$$

If, further, we consider the linear form

$$\varphi = \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n v_n,$$

where the v's are a system of indeterminates, it follows as in the case of formulas (2) and (7) of Art. 176, that

$$N(\varphi) = N(\mathfrak{m})V,$$

where V is a composite unit form of the realm whose determinant is equal to the fundamental invariant D.

Since φ may be transformed into the linear form

$$f = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n$$

through the relations

$$u_i = a_{1i}v_1 + a_{2i}v_2 + \cdots + a_{ni}v_n \quad (i = 1, 2, \cdots, n), \tag{1}$$

we have the equality of the two unit-forms

$$U = V.$$

In other words *the form U is transformed into the form V through the substitutions (1).* Two forms for which this condition exists are said to be *equivalent.* Accordingly, *all composite unit-forms to which the different bases of the ideal* $\mathfrak{m}$ *lead, are equivalent to one another; that is, they are forms of the same class.*

Reciprocally, every form of the class in question has its origin in a definite basis of the ideal $\mathfrak{m}$.

For, if V is a unit-form that is equivalent to the unit-form U, the one being transformed into the other by means of the substitutions

$$u_i = a_{1i}v_1 + a_{2i}v_2 + \cdots + a_{ni}v_n \quad (i = 1, 2, \cdots, n)$$

with determinant

$$|a_{ik}| = 1,$$

then the numbers

$$\beta_i = a_{1i}\alpha_1 + a_{2i}\alpha_2 + \cdots + a_{ni}\alpha_n \quad (i = 1, 2, \cdots, n)$$

form a basis of the ideal $\mathfrak{m}$ to which clearly the form V belongs, being the unit-form which has its source in the basis $\beta_1, \beta_2, \cdots, \beta_n$. (See Art. 24.)

More generally, *there belongs to this class of forms the complex of all the composite unit-forms which have their sources in the ideals that are equivalent to* $\mathfrak{m}$.

For, if $\mathfrak{m}' = \beta\mathfrak{m}$ is such an ideal, where β is a number (fractional or integral) of the realm with positive norm, then the products

$$\beta\alpha_1, \beta\alpha_2, \cdots, \beta\alpha_n,$$

being *integers* in $\mathfrak{m}'$, form a basis of $\mathfrak{m}'$. Next, if integral rational values are given to the u's so that the linear form f becomes an integer α of $\mathfrak{m}$, it is seen that the

formula of Art. 176, namely

$$f\tilde{\omega}_i = U_{i1}\alpha_1 + U_{i2}\alpha_2 + \cdots + U_{in}\alpha_n,$$

now becomes

$$\beta\alpha \cdot \omega_i = U_{i1}\beta\alpha_1 + U_{i2}\beta\alpha_2 + \cdots + U_{in}\beta\alpha_n \quad (i=1, 2, \cdots, n),$$

where $\omega_1, \omega_2, \cdots, \omega_n$ form a basis of $\mathfrak{o}$. And instead of the equations (4) of Art. 176, there enter here

$$\beta\alpha_i = g_{i1}\omega_1 + g_{i2}\omega_2 + \cdots + g_{in}\omega_n \quad (i=1, 2, \cdots, n),$$

where the g's are rational integers.

It follows at once that

$$\beta\alpha \cdot \omega_i = \sum_{k,h} U_{ik} g_{kh} \omega_h \qquad (i=1, 2, \cdots, n),$$

from which the value of $N(\beta\alpha)$ is seen to be

$$N(\beta\alpha) = |U_{ik}|\,|g_{kh}| = UN(\beta\mathfrak{m}) = N(\mathfrak{m}')U.$$

Observe that α is any number of the linear form f, which is the content of $\mathfrak{m}$. From this it is seen that to all ideals that are equivalent to $\mathfrak{m}$ there corresponds one and the same composite unit-form U, or an equivalent form. The class of forms in question may accordingly be designated as the class that corresponds to the ideal class. With this is proved the theorem:

To every class of ideals there corresponds a uniquely determined class of composite unit-forms of the realm whose discriminant is the fundamental invariant D. To the transformation of the forms of this class there corresponds the transition from a basis of one of these ideals to another basis, and vice versa.

Among the transformations of one unit-form into another there are those which transform such a form into itself. If the equations

$$u_i = a_{1i}v_1 + a_{2i}v_2 + \cdots + a_{ni}v_n \qquad |a_{ik}| = 1 \quad (i=1, 2, \cdots, n)$$

present such a transformation, so that V is transformed

into the same form as U, it is seen that

$$N(\beta_1 u_1+\beta_2 u_2+\cdots+\beta_n u_n)=N(\alpha_1 u_1+\alpha_2 u_2+\cdots+\alpha_n u_n).$$

By giving to the u's system of rational integral values including 0, it is clear, if

$$f=\alpha_1 u_1+\alpha_2 u_2+\cdots+\alpha_n u_n=\alpha$$

for such a system of values, that also

$$\varphi=\beta_1 u_1+\beta_2 u_2+\cdots+\beta_n u_n=\beta$$

for the same system, where α and β are two integers of $\mathfrak{m}$, such that $N(\alpha)=N(\beta)$. It follows that $\beta=\epsilon\alpha$, where

$$N(\epsilon)=+1.$$

In particular, it is seen that

$$\beta_1=\epsilon_1\alpha_1,\ \beta_2=\epsilon_2\alpha_2,\ \cdots,\ \beta_n=\epsilon_n\alpha_n,$$

where

$$N[\epsilon_i]=1 \qquad (i=1, 2, \cdots, n).$$

And it is clear that the n integers $\beta_1, \beta_2, \cdots, \beta_n$ form a basis of $\mathfrak{m}$. Due to the fact that for every unit ϵ with positive norm, the integers

$$\beta_1=\epsilon\alpha_1,\ \beta_2=\epsilon\alpha_2,\ \cdots,\ \beta_n=\epsilon\alpha_n$$

offer a basis of the kind required, it is seen that, corresponding to the infinitude of units ϵ, there exist an infinite number of transformations of the unit-form U into itself. With this it has not been determined whether such are the only transformations by which a unit-form is transformed into itself. There remains also the question to be answered whether reciprocally *to each class of composite unit-forms of the realm whose fundamental invariant is D, there corresponds a uniquely determined class of ideals or a multiplicity of such classes of the realm.*

That to every such unit-form corresponds an ideal, and therefore to a class of unit-forms there corresponds a class of ideals of the realm, is known from Art. 176. And it is to be observed that the results established in

Art. 176 for any linear factor U_1 say of U may be derived for any other linear factor, which consists of numbers of the same realm; and it is seen that to the same unit-form or to its class there will correspond as many ideal classes of the realm (whether they be different or not) as there are ideal classes among the conjugate realms that are identical with the given class. Whether there are ideal classes which are in fact different from one another remains to be determined.

With this is proved the theorem:[1] *If U is a primitive form, composite in the realm $\Re$ of degree n, but not factorable in any realm of lower degree, there exists in $\Re$ at least one and at most n ideal classes to which the form U belongs.*

ART. **180.** Parallel with the equivalence of the ideals of a realm, and the composite forms which have their source in it, there corresponds to the multiplication of ideals and the composition[2] of their classes the composition of composite forms and their classes. To set this into evidence, let

$$\mathfrak{a}=(\alpha_1, \alpha_2, \cdots, \alpha_n), \qquad \mathfrak{b}=(\beta_1, \beta_2, \cdots, \beta_n)$$

be two ideals of the realm and let $\mathfrak{c}=\mathfrak{a}\cdot\mathfrak{b}$, so that

$$\mathfrak{c}=(\cdots, \alpha_i\beta_k, \cdots)=(\gamma_1, \gamma_2, \cdots, \gamma_n),$$

where $\mathfrak{c}$ consists of the n^2 elements

$$\alpha_i\beta_k \qquad (i=1, 2, \cdots; k=1, 2, \cdots, n),$$

and where

$$\gamma_i \qquad (i=1, 2, \cdots, n)$$

are the basal elements of $\mathfrak{c}$. It follows, on the one hand that

$$(1) \qquad \alpha_i\beta_k=a_1^{(i,k)}\gamma_1+a_2^{(i,k)}\gamma_2+\cdots+a_n^{(i,k)}\gamma_n,$$

where

$$a_l^{(i,k)} \qquad (l=1, 2, \cdots, n)$$

[1] See Hilbert, *Die Theorie der alg. Zahlkörper*, Satz 59.
[2] Dirichlet-Dedekind, *Zahlentheorie*, § 182, 4th Edition.

are rational integers; and on the other hand that

$$\gamma_h = c_h^{(1,1)}\alpha_1\beta_1 + \cdots + c_h^{(i,k)}\alpha_i\beta_k + \cdots + c_h^{(n,n)}\alpha_n\beta_n \qquad (h=1, 2, \cdots, n), \tag{2}$$

where $c_h^{(i,k)}$ are rational integers.

Substituting the expressions (1) in (2) and observing that the γ's are linearly independent, it is seen that

$$\sum_{i,k} a_h^{(i,k)} c_{h'}^{(i,k)} = e_{h,h'}, \tag{3}$$

where

$$e_{h,h'} = 1 \text{ or } 0,$$

according as h, h' are equal or unequal.

Note that the expressions (3) are the elements of the determinant D_3 which arises through the multiplication of the determinants D_1 and D_2 of the linear forms (1) and (2). Since $D_3 = 1$, it is seen that the coefficients of the determinants D_1 have 1 as their greatest common divisor, the same being true of the coefficients of D_2.

Next write

$$\begin{cases} f = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n, \\ \varphi = \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n v_n, \\ \psi = \gamma_1 w_1 + \gamma_2 w_2 + \cdots + \gamma_n w_n, \end{cases} \tag{4}$$

where

$$N(f) = N(\mathfrak{a})U, \qquad N(\varphi) = N(\mathfrak{b})V, \qquad N(\psi) = N(\mathfrak{c})W, \tag{5}$$

U, V and W being unit-forms. Due to (1) it is seen that

$$f \cdot \varphi = \sum_{i,k} \alpha_i\beta_k u_i v_k = \sum_{i,k,h} a_h^{(i,k)} u_i v_k \gamma_h.$$

If we give to the indeterminates $w_1, w_2, \cdots, w_n$ the values

$$w_h = \sum_{i,k} a_h^{(i,k)} u_i v_k \qquad (h=1, 2, \cdots, n), \tag{6}$$

and write

$$\psi = f \cdot \varphi = w_1\gamma_1 + w_2\gamma_2 + \cdots + w_n\gamma_n,$$

it follows that

$$N(\psi) = N(f)N(\varphi);$$

and at the same time, since

$$N(\mathfrak{c}) = N(\mathfrak{a})N(\mathfrak{b}),$$

we further have

$$W = U \cdot V.$$

And that is, if the relations (6) exist among the indeterminates w, u and v, with the further restrictions that

$$D_3 = D_1 \cdot D_2 = 1,$$

then the unit-form W, which has its source in the ideal-product $\mathfrak{c} = \mathfrak{a} \cdot \mathfrak{b}$, becomes the product $U \cdot V$, where U and V are respectively the unit-forms that have their sources in the ideals $\mathfrak{a}$ and $\mathfrak{b}$. Accordingly, the unit-form W is said to be compounded out of the unit-forms U and V.

It may be observed that the three forms U, V and W are uniquely connected through the bilinear substitution (6). For, if due to this substitution there exists among the linear forms the relation

$$\psi = f \cdot \varphi,$$

it follows that

$$f \frac{\partial \varphi}{\partial v_i} = \frac{\partial \psi}{\partial v_i},$$

or

$$f\beta_i = \sum_h \frac{\partial w_h}{\partial v_i} \gamma_h.$$

Observe next that the integers γ which are the basal elements of $\mathfrak{c}$ are also integers in the ideals that are the divisors of $\mathfrak{c}$, and that is, they are integers in $\mathfrak{b}$ and in $\mathfrak{a}$. Accordingly, we may write

$$\gamma_h = b_{h1}\beta_1 + b_{h2}\beta_2 + \cdots + b_{hn}\beta_n \quad (h = 1, 2, \cdots, n),$$

where the b_{hk} are rational integers, and where the determinant

$$|b_{ik}| = (\mathfrak{b}, \mathfrak{c}) = (\mathfrak{o}\mathfrak{b}, \mathfrak{a}\mathfrak{b}) = (\mathfrak{o}, \mathfrak{a}) = N(\mathfrak{a}).$$

It follows that

$$f\beta_i = \sum_{h,k} \frac{\partial w_h}{\partial v_i} b_{hk}\beta_k \qquad (i = 1, 2, \cdots, n).$$

From these n equations (see Vol. I, Art. 59) it is seen

that

$$N(f)=\left|\frac{\partial w_h}{\partial v_i}\right|\cdot|b_{h,k}|=\left|\frac{\partial w_h}{\partial v_i}\right|N(\mathfrak{a});$$

or from (5)

$$U=\left|\frac{\partial w_h}{\partial v_i}\right|.$$

Similarly, it follows that

$$V=\left|\frac{\partial w_h}{\partial u_i}\right| \qquad \text{and} \qquad W=U\cdot V=\left|\frac{\partial w_h}{\partial v_i}\right|.\left|\frac{\partial w_h}{\partial u_i}\right|.$$

It may be proved that as the unit-form W is compounded of the forms U and V, the class to which W belongs is compounded of the classes to which U and V belong, since systems of forms which are equivalent to U and V must lead through the relations given above, to forms equivalent to W.

ART. 181. The composite forms which have been treated are not the only ones that belong to a realm of the nth degree. It was seen [Art. 176, formula (14)] that there are also forms whose discriminant are not equal to the fundamental invariant of the realm, but are equal to this invariant multiplied by the square of a rational integer. We shall next show that in every order-modul of the realm there exists a category of composite forms.

Let $\mathfrak{o}_1$ be a definite order-modul of the realm, and let the modul

$$\mathfrak{m}=[\alpha_1, \alpha_2, \cdots, \alpha_n]$$

be an ideal of $\mathfrak{o}_1$. It was seen that if $\mathfrak{a}$ is any ideal of $\mathfrak{o}$ that the order-modul $\mathfrak{a}^0=\frac{\mathfrak{a}}{\mathfrak{a}}$ is equal to $\mathfrak{o}$ (Art. 4). Similarly here, the order-modul $\mathfrak{m}^0$ is equal to

$$\mathfrak{o}_1=[\tilde{\omega}_1, \tilde{\omega}_2, \cdots, \tilde{\omega}_n].$$

If further we write

(1) $$\alpha_i=g_{1i}\omega_1+g_{2i}\omega_2+\cdots+g_{ni}\omega_n \quad (i=1, 2, \cdots, n),$$

where $\omega_1, \omega_2, \cdots, \omega_n$ are the basal elements of $\mathfrak{o}$, then is $|g_{ik}|$ with positive sign $=(\mathfrak{o}_1, \mathfrak{m}) = N'(\mathfrak{m}) = N(\mathfrak{om})$. Instead of the equation (7) of Art. 176, we have here

$$N(f) = N(\mathfrak{o}\mathfrak{m})U. \tag{2}$$

Observing formula (13) of Art. 176, it is seen that

$$\Delta[N(f)] = \Delta(\mathfrak{m}) = |g_{ik}|^2 \Delta(\mathfrak{o}_1).$$

From (2) we further have

$$\Delta[N(f)] = |g_{ik}|^2 \Delta(U).$$

It follows that

$$\Delta(U) = \Delta(\mathfrak{o}_1) = N(\mathfrak{o}_1)^2 D,$$

where D is the fundamental invariant of the fixed realm.

With this it is proved that *corresponding to every ideal in* $\mathfrak{o}_1$ *there exists a composite form* U *of the realm, whose discriminant is equal to* $N(\mathfrak{o}_1)^2 \cdot D$.

ART. **182.** To prove that U of the preceding article is a unit-form, we must prove [1] a theorem which has the same significance for ideals in $\mathfrak{o}_1$, as the theorem of Art. 66, Example 1 has for ideals in $\mathfrak{o}$.

THEOREM. *If* $\mathfrak{a}$ *is any ideal in* $\mathfrak{o}_1$, *there exists a second ideal* $\mathfrak{b}$ *in* $\mathfrak{o}_1$, *such that* $\mathfrak{ab}$ *is a principal ideal of* $\mathfrak{o}_1$; *and further,* $\mathfrak{b}$ *is relatively prime to* $\mathfrak{n}$, *where* $\mathfrak{n}$ *is any given ideal (or modul) in* $\mathfrak{o}_1$, *which satisfies the equation* $\mathfrak{o}_1\mathfrak{n} = \mathfrak{n}$.

To prove this theorem, observe that $\mathfrak{on}$ is an ideal in $\mathfrak{o}$, and put $\mathfrak{on} = \mathfrak{n}'\mathfrak{f}'$, where $\mathfrak{f}'$ contains all the ideal factors of $\mathfrak{n}$ which are divisors of the ring-leader $\mathfrak{f}$, so that $\mathfrak{n}'$ is relatively prime to $\mathfrak{f}$. Due to the theorem mentioned in Art. 177, there exists a realm ideal $\mathfrak{c}$ which is relatively prime to $\mathfrak{n}'$ and when compounded with the realm ideal $\mathfrak{oa}$ is such that $\mathfrak{oac} = \mathfrak{o}\gamma$, where $\mathfrak{o}\gamma$ is a principal ideal in $\mathfrak{o}$; and that is,

$$\mathfrak{ac} = \mathfrak{o}\gamma.$$

[1] See Dedekind, *Festschrift zur Säkularfeier des Geburtstages von C. F. Gauss*, Braunschweig, 1877, p. 28; *Werke*, Vol. I, p. 132.

Since

$$\mathfrak{c}+\mathfrak{n}'=\mathfrak{o},$$

it follows, when multiplied by $\mathfrak{oa}$, that

(1) $$\mathfrak{o}\gamma+\mathfrak{oan}'=\mathfrak{oa}.$$

By definition

$$\mathfrak{a}+\mathfrak{f}=\mathfrak{o}_1,$$

and, as $\mathfrak{n}'$ is also relatively prime to $\mathfrak{ff}'$, it follows that

$$\mathfrak{oan}'+\mathfrak{ff}'=\mathfrak{o}.$$

It is accordingly possible to determine integers ω such that

(2) $\omega\equiv\gamma \pmod{\mathfrak{oan}'}$ and $\omega\equiv 1 \pmod{\mathfrak{ff}'}$

are true simultaneously. The ω's form a class of congruent integers that are congruent (mod. $\mathfrak{oan}'-\mathfrak{ff}'$) and consequently (Vol. I, Art. 143) there exists an ω with *positive* norm that satisfies the congruences (2).

Due to the second of these congruences ω is congruent to 1 (mod. $\mathfrak{f}$); and since this congruence exists also (mod. $\mathfrak{o}_1$), it follows that ω is an integer in $\mathfrak{o}_1$, since 1 belongs to $\mathfrak{o}_1$.

With this it is proved that $\mathfrak{o}_1\omega$ *is a principal ideal of the order-modul* $\mathfrak{o}_1$. Having regard to the first of the congruences (2), it is seen that formula (1) may be written

(3) $$\mathfrak{o}\omega+\mathfrak{oa}\cdot\mathfrak{n}'=\mathfrak{oa}.$$

And from this it is seen that $\mathfrak{o}\omega$ is divisible by $\mathfrak{oa}$, so that

(4) $$\mathfrak{o}\omega=\mathfrak{oa}\cdot\mathfrak{d},$$

where $\mathfrak{d}$ is a realm ideal which like $\mathfrak{o}\omega$ is relatively prime to $\mathfrak{f}$. It follows (Art. 166) that there exists an ideal $\mathfrak{b}$ in $\mathfrak{o}_1$, such that

$$\mathfrak{ob}=\mathfrak{d}.$$

Hence, from (4), we have

$$\mathfrak{oo}_1\omega=\mathfrak{oab},$$

where $\mathfrak{o}_1\omega$, $\mathfrak{a}$, $\mathfrak{b}$ are all ideals in $\mathfrak{o}_1$. From this it was proved (Arts. 168 and 14) that

$$\mathfrak{o}_1\omega = \mathfrak{a}\mathfrak{b}. \tag{5}$$

To prove the second part of the theorem, namely, that $\mathfrak{b}$ is relatively prime to $\mathfrak{n}$, observe that from (3)

$$\mathfrak{o}\mathfrak{a}\mathfrak{b} + \mathfrak{o}\mathfrak{a}\mathfrak{n}' = \mathfrak{o}\mathfrak{a}, \tag{6}$$

or

$$\mathfrak{o}\mathfrak{a}(\mathfrak{o}\mathfrak{b} + \mathfrak{n}') = \mathfrak{o}\mathfrak{a}\mathfrak{o},$$

an equation in realm ideals from which it follows that

$$\mathfrak{o}\mathfrak{b} + \mathfrak{n}' = \mathfrak{o}.$$

This equation shows that $\mathfrak{o}\mathfrak{b}$ is relatively prime to $\mathfrak{n}'$. Further, from (5) and the second congruence in (2) it is seen that $\mathfrak{o}\mathfrak{b}$ is prime to ff' and therefore also to $\mathfrak{f}\mathfrak{f}' \cdot \mathfrak{n}' (= \mathfrak{o}\mathfrak{n}\mathfrak{f})$, a result which is expressed through the relation

$$\mathfrak{o}\mathfrak{b} + \mathfrak{o}\mathfrak{n}\mathfrak{f} = \mathfrak{o},$$

or

$$\mathfrak{o}(\mathfrak{b} + \mathfrak{n}\mathfrak{f}) = \mathfrak{o} = \mathfrak{o}\mathfrak{o}_1. \tag{7}$$

To prove that $\mathfrak{b} + \mathfrak{n}\mathfrak{f}$ is an ideal in $\mathfrak{o}_1$, observe *first* that

$$\mathfrak{o}_1(\mathfrak{b} + \mathfrak{n}\mathfrak{f}) = \mathfrak{b} + \mathfrak{n}\mathfrak{f},$$

and, secondly

$$(\mathfrak{b} + \mathfrak{n}\mathfrak{f}) + \mathfrak{f} = (\mathfrak{b} + \mathfrak{f}) + \mathfrak{n}\mathfrak{f} = \mathfrak{o}_1 + \mathfrak{n}\mathfrak{f} = \mathfrak{o}_1.$$

It then follows from (7) that

$$\mathfrak{b} + \mathfrak{n}\mathfrak{f} = \mathfrak{o}_1;$$

and since

$$\mathfrak{n}\mathfrak{f} > \mathfrak{n}\mathfrak{o}_1 = \mathfrak{n},$$

we have, finally,

$$\mathfrak{b} + \mathfrak{n} = \mathfrak{o}_1,$$

with which is proved the theorem.

To show that U is a unit-form, let k be any rational integer and observe that $\mathfrak{o}_1 k$ is an ideal. In the theorem above put

$$\mathfrak{a} = \mathfrak{m}.$$

It is seen that an ideal $\mathfrak{b}$ may be found in $\mathfrak{o}_1$, such that

$$\mathfrak{m}\mathfrak{b} = \mathfrak{o}_1\omega,$$

where $\mathfrak{o}_1\omega$ is a principal ideal in $\mathfrak{o}_1$, and at the same time

$$\mathfrak{b} + \mathfrak{o}_1 k = \mathfrak{o}_1.$$

It follows that

$$\mathfrak{o}\mathfrak{b} + \mathfrak{o}k = \mathfrak{o},$$

and that is, $\mathfrak{o}\mathfrak{b}$ is relatively prime to k as is also $N(\mathfrak{o}\mathfrak{b})$.

From equation (3) above it is seen that ω is an integer of $\mathfrak{o}\mathfrak{m}$. As ω is also an integer of $\mathfrak{o}_1$, it is seen that ω is found in $\mathfrak{o}_1 - \mathfrak{o}\mathfrak{m}$, and that is, in $\mathfrak{m}$. Hence (see formula (5)), we may write

$$\mathfrak{o}_1\omega = \mathfrak{m}\mathfrak{b} \qquad \text{and therefore} \qquad \mathfrak{o}\omega = \mathfrak{o}\mathfrak{m} \cdot \mathfrak{o}\mathfrak{b}.$$

Taking the norm of this expression, it is seen that

$$N(\omega) = \pm N(\mathfrak{o}\omega) = \pm N(\mathfrak{o}\mathfrak{m}) N(\mathfrak{o}\mathfrak{b}).$$

On the other hand, from (2) of the preceding article, when the u's have been chosen so that f becomes ω, we have

$$N(\omega) = N(\mathfrak{o}\mathfrak{m}) U.$$

It follows that

$$U = \pm N(\mathfrak{o}\mathfrak{b}),$$

which from above is relatively prime to k.

With this it is seen that the u's in U may be so chosen that U is relatively prime to any rational integer k. And from this it follows that the greatest common divisor of the coefficients of U must be unity; and that is, U is a unit-form.

With the proof of the above theorems it becomes evident that the same theorems that exist for the equivalence of ideals, the composition of forms, etc. in $\mathfrak{o}$ are at once applicable in any order-modul $\mathfrak{o}_1$.

ART. **183.** It may be observed further that there are other composite forms of the nth degree besides those already considered. For the modul $\mathfrak{m} = [\alpha_1, \alpha_2, \cdots, \alpha_n]$

consisting of integers of the given realm need not be an ideal either of the realm or of the order-modul and still the formula (7) of Art. 176, and that is

$$N(f) = |r_{ik}|\,U, \tag{1}$$

presents a composite form U of the fixed realm which *corresponds* to the modul $\mathfrak{m}$. For, from the relations (4) of Art. 176, namely,

$$\alpha_i = r_{i1}\tilde{\omega}_1 + r_{i2}\tilde{\omega}_2 + \cdots + r_{in}\tilde{\omega}_n \quad (i=1, 2, \cdots, n), \tag{2}$$

it is seen, if we again put

$$f = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n,$$

that

$$\Delta[N(f)] = \Delta(\mathfrak{m}) = |r_{ik}|^2 \Delta(\mathfrak{m}^0),$$

where $\mathfrak{m}^0$ is the order-modul

$$\frac{\mathfrak{m}}{\mathfrak{m}} = [\tilde{\omega}_1, \tilde{\omega}_2, \cdots, \tilde{\omega}_n].$$

From (1) it follows that

$$\Delta[N(f)] = |r_{ik}|^2 \Delta(U).$$

From these two relations it is seen that

$$\Delta(U) = \Delta(\mathfrak{m}^0) = N(\mathfrak{m}^0)^2 D.$$

As in the cases already considered, there also exist here analogous theorems regarding the equivalence of the forms U that correspond to the different moduls. For, we may define for integral moduls the notion of *equivalence* in the same way as has been done for ideals, in that two n-termed moduls $\mathfrak{m}$ and $\mathfrak{m}'$ of the fixed realm are said to be *equivalent*, if there is a number β with positive norm for which $\mathfrak{m}' = \beta\mathfrak{m}$. Accordingly, moduls are distributed into classes, equivalent moduls belonging to the same class. Evidently, all moduls of the same class have the same quotient $\mathfrak{m}^0$, and that is, they have the same order-modul. For, if ω is any integer of $\mathfrak{m}^0$, it follows that $\omega\mathfrak{m} > \mathfrak{m}$ and therefore also $\omega\beta\mathfrak{m} > \beta\mathfrak{m}$, or

$\omega\mathfrak{m}' > \mathfrak{m}'$. From this it is seen that ω is an integer of $(\mathfrak{m}')^0$, and reciprocally.

Further, if $\mathfrak{a}$ goes through all moduls of a class A, and if $\mathfrak{b}$ goes through all moduls of a class B, the product $\mathfrak{ab}$ will belong to a definite class C, which class, as in the case of ideals, is said to be compounded of the two classes A and B.

It is clear that the same theorems must exist for the equivalence and composition of the composite unit-forms U which have their sources in these moduls as are true of the theorems proved in the previous articles.

A final remark may be added. In formula (12), Art. 176, was derived the relation

$$\Delta[N(f)] = \Delta(\mathfrak{m}) = |a_{ik}|^2 N(\mathfrak{a})^2 D,$$

or

$$D|a_{ik}|^2 = \frac{\Delta(\mathfrak{m})}{N(\mathfrak{a})^2}. \tag{3}$$

It may be proved that *this quotient is an invariant of the class to which the modul* $\mathfrak{m}$ *belongs.*

For, consider the modul $\mathfrak{m} = [\alpha_1, \alpha_2, \cdots, \alpha_n]$, where $\alpha_1, \alpha_2, \cdots, \alpha_n$ are integers of a fixed realm. The associate ideal is $\mathfrak{a} = (\alpha_1, \alpha_2, \cdots, \alpha_n) = [\beta_1, \beta_2, \cdots, \beta_n]$, where the β's in the square brackets form a basis of $\mathfrak{a}$. (Art. 2; Vol. I, Art. 114.) Let $\mathfrak{m}' = \beta\mathfrak{m}$ be a modul equivalent to $\mathfrak{m}$. Since by hypothesis the moduls are to consist of integers of the fixed realm, the basal elements $\beta\alpha_1, \beta\alpha_2, \cdots, \beta\alpha_n$ of $\mathfrak{m}'$ are integral. There corresponds an ideal $\mathfrak{a}'$ which is equivalent to $\mathfrak{a}$ namely,

$$\mathfrak{a}' = \beta\mathfrak{a} = (\beta\alpha_1, \beta\alpha_2, \cdots, \beta\alpha_n).$$

Observe further that $\beta\beta_1, \beta\beta_2, \cdots, \beta\beta_n$ form an integral basis of $\mathfrak{a}'$, and note that there exist the same relations between the basal elements of $\mathfrak{m}'$ and $\mathfrak{a}'$ on the one hand as between $\mathfrak{m}$ and $\mathfrak{a}$ on the other. Accordingly, the left

hand side of (3) remains unchanged. And with this is proved the assertion that

$$\frac{\Delta(\mathfrak{m}')}{N(\mathfrak{a}')^2}=\frac{\Delta(\mathfrak{m})}{N(\mathfrak{a})^2}.$$

The quotient $\frac{\Delta(\mathfrak{m})}{N(\mathfrak{a})^2}$, which is an innate property of $\mathfrak{m}$, is sometimes called the *discriminant of the class of moduls to which* $\mathfrak{m}$ *belongs*.

Finally, it may be remarked that

$$\frac{(\mathfrak{o}_1, \mathfrak{m})}{(\mathfrak{m}, \mathfrak{o}_1)}=\sqrt{\frac{\Delta(\mathfrak{m})}{\Delta(\mathfrak{o}_1)}}.$$

This follows from formula (5) of Art. 176, namely, $|r_{ik}|$, taken with positive value, $=\frac{(\mathfrak{o}_1, \mathfrak{m})}{(\mathfrak{m}, \mathfrak{o}_1)}$ with the relation found above, namely,

$$\Delta(\mathfrak{m})=|r_{ik}|^2\Delta(\mathfrak{o}_1), \qquad \text{where} \qquad \mathfrak{o}_1=\frac{\mathfrak{m}}{\mathfrak{m}}.$$

It is observed that this is only a special case of the relation

$$\frac{(\mathfrak{m}', \mathfrak{m})}{(\mathfrak{m}, \mathfrak{m}')}=\sqrt{\frac{\Delta(\mathfrak{m})}{\Delta(\mathfrak{m}')}},$$

which exists in general for two moduls $\mathfrak{m}$ and $\mathfrak{m}'$ (see Vol. I, Art. 167).

CHAPTER XII

RELATIVE REALMS. SUB–REALMS. SUPER–REALMS

ART. **184. Definitions.** The conception of norm, discriminant, different, etc., which have been introduced in the previous chapters are susceptible of extensive generalizations. Instead of considering an algebraic realm Ω, we may take here a realm $\mathfrak{R} = \mathfrak{R}(\theta, \Theta)$. If $\mathfrak{R}$ is a realm of degree N, which contains all the numbers of a realm $\mathfrak{k} = \mathfrak{R}(\theta)$ of degree n, then $\mathfrak{k}$ is a *sub-realm* of $\mathfrak{R}$, while $\mathfrak{R}$ is a *super-realm* of $\mathfrak{k}$. The realm $\mathfrak{R}$ is called the *relative realm* with respect to $\mathfrak{k}$.

Let Θ be a number which determines $\mathfrak{R}$, and among the infinite number of equations with algebraic integral coefficients in $\mathfrak{k}$, let the following equation of degree r

$$\Theta^r + \alpha_1\Theta^{r-1} + \cdots + \alpha_r = 0 \tag{1}$$

be that one of the lowest degree. The quantities $\alpha_1, \cdots, \alpha_r$ are algebraic integers in $\mathfrak{k}$. The integer r is called the *relative degree* of $\mathfrak{R}$ with respect to $\mathfrak{k}$, and $N = r \cdot n$ (note Vol. I, Art. 68). The equation (1) is irreducible in the realm of rationality $\mathfrak{k}$.

If $\Theta', \cdots, \Theta^{(r-1)}$ are the other $r-1$ roots of the equation (1), these quantities are called the *relative conjugate* numbers to Θ; and the realms $\mathfrak{R}', \cdots, \mathfrak{R}^{(r-1)}$ are the *relative conjugate realms to* $\mathfrak{R}$.

The numbers of $\mathfrak{R}$ are denoted by capital Greek letters.

If A is an arbitrary integer in $\mathfrak{R}$, and if (Vol. I, Art. 44)

$$A = \gamma_1 + \gamma_2\Theta + \cdots + \gamma_r\Theta^{r-1},$$

where the γ's are numbers of $\mathfrak{k}$, the integers

$$A' = \gamma_1 + \gamma_2\Theta' + \cdots + \gamma_r\Theta'^{r-1},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$A^{(r-1)} = \gamma_1 + \gamma_2\Theta^{(r-1)} + \cdots + \gamma_r[\Theta^{(r-1)}]^{r-1},$$

are called the *relative conjugate integers* to A.

If $\mathfrak{J}$ is the ideal $(A_1, \cdots, A_r)$, then the ideals which are derived from this ideal through the substitutions

$$s' = (\Theta : \Theta'), \cdots, s^{(r-1)} = (\Theta : \Theta^{(r-1)}),$$

and that is, the ideals

$$\mathfrak{J}' = (A_1', \cdots, A_r'), \cdots, \mathfrak{J}^{(r-1)} = (A_1^{(r-1)}, \cdots, A_{r-1}^{(r-1)})$$

are called the *relative conjugate ideals* to $\mathfrak{J}$.

If $\alpha_1, \cdots, \alpha_s$ are arbitrary integers of $\mathfrak{k}$, and if they constitute an ideal $\mathfrak{i} = (\alpha_1, \cdots, \alpha_s)$, they also determine an ideal $\mathfrak{J} = (\alpha_1, \cdots, \alpha_s)$ in $\mathfrak{R}$. That the ideal $\mathfrak{i}$ is not to be regarded as different from $\mathfrak{J}$ is seen from the following consideration: Let $\alpha_1, \cdots, \alpha_s$ and $\alpha_1^*, \cdots, \alpha_s^*$ be integers in $\mathfrak{k}$ such that in $\mathfrak{R}$ the ideals $\mathfrak{J} = (\alpha_1, \cdots, \alpha_s)$ and $\mathfrak{J}^* = (\alpha_1^*, \cdots, \alpha_s^*)$ are equal. Then in $\mathfrak{k}$ the two ideals

$$\mathfrak{i} = (\alpha_1, \cdots, \alpha_s) \qquad \text{and} \qquad \mathfrak{i}^* = (\alpha_1^*, \cdots, \alpha_s^*)$$

are also equal. For, since $\mathfrak{J} = \mathfrak{J}^*$, it follows, if α^* is one of the integers $\alpha_1^*, \cdots, \alpha_s^*$, that

$$\alpha^* = A_1\alpha_1 + \cdots + A_s\alpha_s,$$

where $A_1, \cdots, A_s$ are algebraic integers in $\mathfrak{R}$.

Forming the relative norm of both sides of this equation, it is seen that in $\mathfrak{k}$

$$\alpha^{*r} = \tau_1\alpha_1^r + \tau_2\alpha_1^{r-1}\alpha_2 + \cdots,$$

where $\tau_1, \tau_2, \cdots$ are algebraic integers in $\mathfrak{k}$; and that is, α^{*r} is divisible by $\mathfrak{i}^r$; and consequently, α^* is divisible by $\mathfrak{i}$. It follows that $\mathfrak{i}^*$ is divisible by $\mathfrak{i}$; and, reversing the process, $\mathfrak{i}$ is divisible by $\mathfrak{i}^*$, and consequently in $\mathfrak{k}$ the ideal $\mathfrak{i}$ is equal to $\mathfrak{i}^*$.

Reciprocally, an ideal $\mathfrak{J}=(A_1, \cdots, A_s)$ of the realm $\mathfrak{R}$ is also an ideal in $\mathfrak{k}$, when and only when $\mathfrak{J}$ may be expressed at the same time as the greatest common divisor of certain integers $\alpha_1, \cdots, \alpha_s$ of $\mathfrak{k}$.

The product of a number A by its relative conjugate numbers

$$N_{\mathfrak{k}}(A)=AA'\cdots A^{(r-1)}$$

is called the *relative norm* of the number A with respect to the realm of rationality $\mathfrak{k}$.

The relative norm $N_{\mathfrak{k}}$ is a number in $\mathfrak{k}$.

If $\mathfrak{J}=(A_1, \cdots, A_S)$ is an arbitrary ideal in $\mathfrak{R}$, the product of $\mathfrak{J}$ with the conjugate ideals of $\mathfrak{J}$,

$$N_{\mathfrak{k}}(\mathfrak{J})=\mathfrak{J}\cdot\mathfrak{J}'\cdots\mathfrak{J}^{(r-1)}$$

is the relative norm of the ideal $\mathfrak{J}$. This relative norm is an ideal of the realm $\mathfrak{k}$. For, if $U_1, \cdots, U_S$ are indeterminates, the coefficients of the product

$$(A_1U_1+\cdots+A_sU_s)(A_1'U_1+\cdots+A_S'U_S)\cdots(A_1^{(r-1)}U_1+\cdots+A_S^{(r-1)}U_S)$$

being symmetric functions, are algebraic integers in $\mathfrak{k}$ and the content of this expression is the norm $N_{\mathfrak{k}}(\mathfrak{J})$.

The expression

$$\Delta_{\mathfrak{k}}(A)=(A-A')\cdots(A-A^{(r-1)})$$

is a number of the realm $\mathfrak{R}$ and is called the *relative different* of the number A with respect to the realm $\mathfrak{k}$.

The expression

$$D_{\mathfrak{k}}(A)=(A-A')^2(A-A'')^2\cdots(A^{(r-2)}-A^{(r-1)})^2,$$

is called the *relative discriminant* of A, and, as in Vol. I, Art. 63,

$$D_{\mathfrak{k}}(A)=(-1)^{\frac{r(r-1)}{2}}N_{\mathfrak{k}}[\Delta_{\mathfrak{k}}(A)].$$

If $\Omega_1, \Omega_2, \cdots, \Omega_N$ are the N basal elements of all integers

in $\mathfrak{R}$, the elements of this realm (Art. 77) are

$$\mathfrak{F}' = ((\Omega_1 - \Omega'), \cdots, (\Omega_N - \Omega'_N)),$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\mathfrak{F}^{(r-1)} = ((\Omega_1 - \Omega_1^{(r-1)}), \cdots, (\Omega_N - \Omega_N^{(r-1)}));$$

and the ideal (Vol. I, Art. 96)

$$\mathfrak{D}_t = \mathfrak{F}'\mathfrak{F}'' \cdots \mathfrak{F}^{(r-1)}$$

is called the *relative different* of the realm $\mathfrak{R}$ with respect to $\mathfrak{k}$.

Denoting the *fundamental form* in $\mathfrak{R}$ by

$$\Xi = \Omega_1 U_1 + \cdots + \Omega_N U_N,$$

the *relative different* of Ξ is

$$\Delta_t(\Xi) = (\Xi - \Xi') \cdots (\Xi - \Xi^{(r-1)}).$$

And the content of the right-hand side is $\mathfrak{D}_t$, so that

$$\Delta_t(\Xi) = \mathfrak{D}_t.$$

Further, writing

$$F_t(X) = (X - \Xi) \cdots (X - \Xi^{(r-1)}),$$

we have

$$\left[\frac{\partial}{\partial X} F_t(X)\right]_{X=\Xi} = \Delta_t(\Xi),$$

so that $\Delta_t(\Xi)$ is an ideal in $\mathfrak{R}$, although the elements $\mathfrak{F}', \cdots \mathfrak{F}^{(r-1)}$ in general do *not* belong to this realm.

The square of the greatest ideal divisor of all the determinants of the rth order, which can be made by taking any r columns of the matrix

$$\begin{vmatrix} \Omega_1, & \Omega_2, & \cdots, & \Omega_N \\ \Omega'_1, & \Omega'_2, & \cdots, & \Omega'_N \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ \Omega_1^{(r-1)}, & \Omega_2^{(r-1)}, & \cdots, & \Omega_N^{(r-1)} \end{vmatrix},$$

is called the *relative discriminant* of the realm $\mathfrak{R}$ with respect to $\mathfrak{k}$.

It is clear that each of the determinants of the rth order is an algebraic integer in $\mathfrak{k}$, so that the relative discriminant is an ideal of the realm $\mathfrak{k}$. It may be denoted by D_t.

ART. 185. **Properties of the Relative Different and of the Relative Discriminant.** THEOREM. *The relative discriminant of the realm* $\mathfrak{R}$ *with regard to the sub-realm* $\mathfrak{k}$ *is equal to the relative norm of the relative different of* $\mathfrak{R}$ *and that is*

$$D_{\mathfrak{k}} = N_{\mathfrak{k}}(\Delta_{\mathfrak{k}}(\Xi)).$$

Proof. The relative norm of the relative different of $\mathfrak{R}$, that is, of the fundamental form Ξ is

$$N_{\mathfrak{k}}(\Delta_{\mathfrak{k}}(\Xi)) = \pm(\Xi-\Xi')^2(\Xi-\Xi'')^2\cdots(\Xi^{(r-2)}-\Xi^{(r-1)})^2$$

$$= \pm \begin{vmatrix} 1, & \Xi, & \cdots, & \Xi^{r-1} \\ 1, & \Xi', & \cdots, & \Xi'^{r-1} \\ \cdots & \cdots & \cdots & \cdots \\ 1, & \Xi^{(r-1)}, & \cdots, & (\Xi^{(r-1)})^{r-1} \end{vmatrix}^2.$$

Write down (see Art. 76) the relations

$$(1) \quad \begin{cases} 1 = U_{11}\Omega_1 + \cdots + U_{1N}\Omega_N, \\ \Xi = U_{21}\Omega_1 + \cdots + U_{2N}\Omega_N, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \Xi^{r-1} = U_{r1}\Omega_1 + \cdots + U_{rN}\Omega_N, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \Xi^{N-1} = U_{N1}\Omega_1 + \cdots + U_{NN}\Omega_N, \end{cases}$$

substitute them in the first row of the determinant, and take the conjugates of these quantities for the other rows. The square of the resulting determinant has coefficients each of which is divisible by $D_{\mathfrak{k}}$. Reciprocally, observe that the determinant of the N linear expressions in (1) is a unit-form, U say. If we solve for the N quantities, $\Omega_1, \cdots, \Omega_N$ and substitute in the determinant for $D_{\mathfrak{k}}$ of the preceding article, it is seen that the resulting expression multiplied by the rth power of U is divisible by the product

$$(\Xi-\Xi')(\Xi-\Xi'')\cdots(\Xi^{(r-2)}-\Xi^{(r-1)}).$$

From this it follows that

$$N_{\mathfrak{k}}(\Delta_{\mathfrak{k}}(\Xi)) \simeq D_{\mathfrak{k}}.$$

ART. **186.** Form the expression

$$\Pi=(\Xi-(\Omega_1U_1+\cdots+\Omega_NU_N))(\Xi-(\Omega'U_1+\cdots+\Omega'_NU_N))\cdots(\Xi-(\Omega_1^{(r-1)}U_1+\cdots+\Omega_N^{(r-1)}U_N)).$$

The coefficients in this product, when expanded, are algebraic integers in $\mathfrak{k}$. These algebraic integers may be expressed in terms of $\omega_1, \cdots, \omega_n$ and these latter quantities may, as in Art. 76, be expressed through ξ and $u_1, \cdots, u_n$, where small u's are written for large U's in Art. 76.

It is thus seen that Ξ (when written for X) satisfies an equation of the rth degree, say

$$\Phi(X, \xi)=\Phi_0X^r+\Phi_1X^{r-1}+\cdots+\Phi_r=0, \tag{1}$$

where $\Phi_0, \cdots, \Phi_r$ are integral functions in ξ and the indeterminates $u_1, \cdots, u_n, U_1, \cdots, U_N$. Observe also that Φ_0 is a unit-form in $u_1, \cdots, u_n$ which is multiplied in the product Π above, since a unit-form appears in the denominators of the expressions for the ω's through the powers of ξ.

The other roots of (1) are $\Xi', \cdots, \Xi^{(r-1)}$.

Let $\xi^{(h)}$ be one of the $n-1$ fundamental forms that are conjugate to ξ; and denote the roots of the equation

$$\Phi(X, \xi^{(h)})=0 \tag{2}$$

by

$$\Xi_{(h)}, \Xi'_{(h)}, \cdots, \Xi^{(r-1)}_{(h)} \qquad (h=1, 2, \cdots, n).$$

Since ξ satisfies an equation of the nth degree, it is clear that every power of Ξ after multiplication with an integral power of Φ_0 is equal to an integral function of ξ and Ξ which is at most of the $n-1$st degree in ξ and of the $(r-1)$th degree in Ξ and with coefficients that are integral functions in $u_1, \cdots, u_n, U_1, \cdots, U_N$. The realm $\mathfrak{R}$ is of degree N and $\Omega_1, \cdots, \Omega_N$ are the basis of all integers in this realm. Denote the discriminant of this

realm by $D(\mathfrak{R})$, so that

$$D(\mathfrak{R}) = \begin{vmatrix} \Omega_1, & \cdots, & \Omega_N \\ \Omega_1', & \cdots, & \Omega_N' \\ \cdots\cdots & \cdots\cdots & \cdots\cdots \\ \Omega_1^{(N-1)}, & \cdots, & \Omega_N^{(N-1)} \end{vmatrix}^2,$$

and let $D(\mathfrak{f})$ be the discriminant of the realm $\mathfrak{f}$.

THEOREM. *If $D_\mathfrak{r}$ denotes the relative discriminant with respect to $\mathfrak{k}$, then is*

$$D(\mathfrak{R}) = D(\mathfrak{f})^r N_\mathfrak{r}(D_\mathfrak{r}).$$

Proof. Form the determinant Δ of the $N = rn$ order as follows: Let

$$1,\ \Xi, \cdots, \Xi^{r-1},\ \xi, \xi\Xi, \cdots, \xi\Xi^{r-1}, \cdots, \xi^{n-1}, \xi^{n-1}\Xi, \cdots, \xi^{n-1}\Xi^{r-1}$$

be the $N = r \cdot n$ elements of the first row. For the second row change ξ to ξ', the nth row being formed by changing ξ in the first row to $\xi^{(n-1)}$. Then make n additional rows by changing Ξ to Ξ' in the rows already formed. Then change Ξ to Ξ'' for n additional rows; and finally change Ξ to $\Xi^{(r-1)}$ for the last set of r rows.

Observe that this determinant vanishes when for Ξ are written any of the quantities $\Xi', \cdots, \Xi^{(r-1)}$ or when for ξ are written any of the quantities $\xi', \xi'', \cdots, \xi^{(n-1)}$; and further as seen above, this determinant may be replaced by an integral function of degree at most $r-1$ in Ξ and $n-1$ in ξ. It is clear that the discriminant of the fundamental form after it has been multiplied by a power of Φ_0 is divisible by Δ^2.

Next express the elements of Δ linearly through the basal elements $\Omega_1, \cdots, \Omega_N$ as in the scheme found in formulas (1) of Art. 185, and it is seen that

$$\Delta = \begin{vmatrix} \Omega_1, & \cdots, & \Omega_N \\ \Omega_1', & \cdots, & \Omega_N' \\ \cdots\cdots & \cdots\cdots & \cdots\cdots \\ \Omega_1^{(N-1)}, & \cdots, & \Omega_N^{(N-1)} \end{vmatrix} \cdot F,$$

where F is an integral function of $u_1, \cdots, u_n, U_1, \cdots, \dot{U}_N$. And from this it is seen that the numerical factor of the square of Δ is divisible by $D(\mathfrak{R})$. Since, however, Art. 184 the numerical factor of the discriminant of Ξ is equal to $D(\mathfrak{R})$, it follows, reciprocally, that D is divisible by the numerical factor of the square of Δ; and that is, the numerical factor of $\Delta^2 = D(\mathfrak{R})$.

Write

$$D_t = \begin{vmatrix} 1, & \Xi, & \cdots, & \Xi^{r-1} \\ 1, & \Xi', & \cdots, & \Xi'^{r-1} \\ \cdots & \cdots & \cdots & \cdots \\ 1, & \Xi^{(r-1)}, & \cdots, & (\Xi^{(r-1)})^{r-1} \end{vmatrix},$$

$$D_t^{(1)} = \begin{vmatrix} 1, & \Xi_{(1)}, & \cdots, & \Xi_{(1)}^{r-1} \\ 1, & \Xi'_{(1)}, & \cdots, & \Xi'^{(r-1)}_{(1)} \\ \cdots & \cdots & \cdots & \cdots \\ 1, & \Xi_{(1)}^{(r-1)}, & \cdots, & (\Xi_{(1)}^{(r-1)})^{r-1} \end{vmatrix},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$D_t^{(n-1)} = \begin{vmatrix} 1, & \Xi_{(n-1)}, & \cdots, & \Xi_{(n-1)}^{r-1} \\ 1, & \Xi'_{(n-1)}, & \cdots, & \Xi'^{r-1}_{(n-1)} \\ \cdots & \cdots & \cdots & \cdots \\ 1, & \Xi_{(n-1)}^{(r-1)}, & \cdots, & (\Xi_{(n-1)}^{(r-1)})^{r-1} \end{vmatrix},$$

and observe that $D_t \cdot D_t^{(1)} \cdot \cdots \cdot D_t^{(n-1)} = N_t(D_t)$. Expanding the determinant Δ, it is seen that

$$\Delta = \begin{vmatrix} 1, & \xi, & \cdots, & \xi^{n-1} \\ 1, & \xi, & \cdots, & \xi'^{n-1} \\ \cdots & \cdots & \cdots & \cdots \\ 1, & \xi, & \cdots, & (\xi^{n-1})^{n-1} \end{vmatrix}^r \cdot N_t(D_t);$$

and from this follows immediately the theorem to be proved.

This theorem not only shows that the discriminant of a realm is divisible by the discriminant of each of its subrealms, but it also shows to what power the latter discriminant enters as a factor of the former, and it

further reveals the simple meaning of the remaining factor of the super-realm.

ART. **187.** THEOREM. *Each element of the sub-realm* $\mathfrak{k}$ *is equal to the product of certain* r *elements of the super-realm* $\mathfrak{K}$ *as presented through the formula*

$$\begin{aligned}\xi-\xi^{(h)} &\simeq (\Xi-\Xi_{(h)})(\Xi-\Xi'_{(h)})\cdots(\Xi-\Xi^{(r-1)}_{(h)})\\ &\simeq (\Xi-\Xi_{(h)})(\Xi'-\Xi_{(h)})\cdots(\Xi^{(r-1)}-\Xi_{(h)}).\end{aligned}$$

Proof. If

$$F(X)=X^N+F_1X^{N-1}+\cdots+F_N=0$$

is the fundamental equation of the Nth degree of the realm $\mathfrak{K}$, where $F_1, \cdots, F_N$ are integral functions of $U_1, \cdots, U_N$, then (see preceding Art.) there exists the identical equation in X

$$(1)\qquad \Phi_0^n F(X)=\Phi(X,\xi)\Phi(X,\xi')\cdots\Phi(X,\xi^{(n-1)}).$$

The different $\Delta(\Xi)$ of the fundamental form is, due to the fact that

$$\Phi(\Xi,\xi)=0,$$

$$(2)\quad \Delta(\Xi)=\frac{\partial F(\Xi)}{\partial\Xi}=\frac{1}{\Phi_0^n}\frac{\partial\Phi(\Xi,\xi)}{\partial\Xi}\Phi(\Xi,\xi')\cdots\Phi(\Xi,\xi^{(n-1)}).$$

On the one hand, from the preceding article,

$$(3)\qquad \Phi(\Xi,\xi^{(h)})=\Phi_0(\Xi-\Xi_{(h)})(\Xi-\Xi'_{(h)})\cdots(\Xi-\Xi^{(r-1)}_{(h)});$$

and, on the other hand, due to the Mean-Value Theorem,

$$(4)\qquad \Phi(\Xi,\xi^{(h)})=\Phi(\Xi,\xi^{(h)})-\Phi(\Xi,\xi)=(\xi-\xi^{(h)})G^{(h)},$$

where $G^{(h)}$ is an integral algebraic form. It follows from (2) that

$$\Phi_0^n\frac{\partial F(\Xi)}{\partial\Xi}=\frac{\partial\Phi(\Xi,\xi)}{\partial\Xi}(\xi-\xi')\cdots(\xi-\xi^{(n-1)})G'\cdots G^{(n-1)}.$$

If the content of both sides of this equation is taken, it is seen that

$$(5)\qquad \mathfrak{D}=\mathfrak{D}_t\mathfrak{d}\mathfrak{J},$$

where $\mathfrak{D}$ is the different of $\mathfrak{K}$, $\mathfrak{D}_t$ the relative different

of $\mathfrak{R}$ with respect to $\mathfrak{k}$, and $\mathfrak{J}$ the ideal that is the content of the form $G' \cdots G^{(n-1)}$, and $\mathfrak{d}$ is the different of the realm $\mathfrak{k}$. If the norm of both sides of the latter expression is taken, it follows that

$$D(\mathfrak{R}) = N_{\mathfrak{k}}(D_{\mathfrak{k}})\mathfrak{d}^r \text{ Norm } (\mathfrak{J});$$

and, from the preceding article, it is seen that

$$\text{Norm } (\mathfrak{J}) = 1 \qquad \text{and consequently} \qquad \mathfrak{J} = (1).$$

It is thus seen that the forms $G', \cdots, G^{(n-1)}$ are all unit-forms. The proof of the theorem is then found in formulas (3) and (4). From formula (5) is derived at once the important theorem.

THEOREM. *The different $\mathfrak{D}$ of the realm $\mathfrak{K}$ is equal to the product of the relative different $\mathfrak{D}_{\mathfrak{k}}$ of $\mathfrak{K}$ with respect to $\mathfrak{k}$ and the different $\mathfrak{d}$ of the realm $\mathfrak{k}$; and that is,*

$$\mathfrak{D} = \mathfrak{D}_{\mathfrak{k}}\mathfrak{d}.$$

By virtue of this theorem, the behavior of the different upon the passage from the sub-realm to the super-realm is of extreme simplicity; the different of the higher realm is had by multiplying the different of the lower realm by the corresponding relative different.

ART. **188.** In the present theory the treatment of rational numbers has been extended through the introduction of the quadratic, the cubic, and in general the algebraic integers of realms of the nth degree. Other generalizations of this theory may be made in a different direction. It was seen in Vol. I, Arts. 239 ff. that the simplest method of treatment of the usual quadratic and cubic laws of reciprocity was effected through the extension of the realm of natural numbers by the *adjunction* of such quantities as i and $\omega = -\frac{1+i\sqrt{3}}{2}$. For example, a proof of the quadratic law of reciprocity

for rational prime numbers, namely,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

was effected through the adjunction of such quantities as $\sqrt{p}$ and $\sqrt{\pm q}$ to the realm of rational numbers, the law of reciprocity being derived from the properties of the resulting extended realms. (Vol. I, pp. 420 ff.)

In a similar manner, if it is required to find a law of reciprocity for prime numbers or prime ideals of a quadratic realm $\Re(\sqrt{m})$, it is natural, taking this realm as the stock realm, to introduce a more general quadratic realm, a *relative quadratic realm*, and from the properties of this realm seek to derive the laws of reciprocity in question. The generalization of this notion is had through the introduction of relative cubic and, in general, through relative realms of any degree and the study of the properties of these extended realms. As indicated in the introduction, this theory only recently has been developed by Hasse, Takagi, Artin, Ore, and others.

To illustrate what has been said above, we may consider the simplest case, that of the relative quadratic realms which is treated in this chapter. It is given by Hilbert, *Math. Ann.*, Bd. 51, pp. 1–127; see also Sommer, *Vorlesungen über Zahlentheorie*, pp. 293 et seq. Other references are the Göttingen dissertations of Dorrie (1898), Ruckle (1901), R. Fueter (1903) and numerous papers by Furtwängler in the *Abh.* and *Nach. von der Kgl. Ges. der Wissenschaften zu Göttingen* of the same time, and in particular, the *Math. Ann.*, Bd. 63. Finally attention is called to the frequently mentioned *Göttingen Dissertation* of Leigh Reid, Gött. 1899, and W. Hasse, *Deutsch. math. Vereinigung*, 1930. Numerous other references are found in the *Report of Algebraic Numbers* by Dickson, Mitchell, Vandiver, and Wahlin, p. 20.

ART. **189. Fundamental Conceptions and Definitions.**[1] Let $\Re(\sqrt{m})$ be any given quadratic realm, in which the rational integer m is free from squared factors, and let μ be any integer of this realm which does not contain, as a factor, the square of an integer of the realm and which is different from 0, 1, and m. Further, let α and β run through all the numbers (integral or fractional) of the realm $\Re(\sqrt{m})$. The complex (collectivity) of all the numbers $\alpha+\beta\sqrt{\mu}$ constitute a new realm $\Re(\sqrt{m};\ \sqrt{\mu})$ in the same sense as hitherto used, since the sum, difference, product and quotient of any two numbers of the form $\alpha+\beta\sqrt{\mu}$ is a number of this form.

Every number $A=\alpha+\beta\sqrt{\mu}$ of this realm satisfies a quadratic equation of the form

$$x^2-2\alpha x+\alpha^2-\beta^2\mu=0,$$

whose coefficients belong to the stock-realm $\Re(\sqrt{m})$. Accordingly, the numbers of the realm $\Re(\sqrt{m};\ \sqrt{\mu})$ are called *relatively quadratic* with respect to $\Re(\sqrt{m})$. The realm $\Re(\sqrt{m};\ \sqrt{\mu})$ is called the *relative realm* or *upper realm* with regard to $\Re(\sqrt{m})$; and since $\Re(\sqrt{m};\ \sqrt{\mu})$ on the other hand contains all the numbers of the realm $\Re(\sqrt{m})$, the latter is called the *lower realm*. The terms *sub-* and *super-* may be affixed to *realm* to denote the two realms in question. It is clear that the realm $\Re(\sqrt{m};\ \sqrt{\mu})$ is related to the stock-realm $\Re(\sqrt{m})$ in the same way that $\Re(\sqrt{m})$ is related to the realm of rational numbers.

In the sequel we shall consider the properties of integers (defined below) of the relative realms.

Two numbers $A=\alpha+\beta\sqrt{\mu}$ and $A'=\alpha-\beta\sqrt{\mu}$ are said to be *relatively conjugate*. It is seen that A' is derived from A by the substitution of $-\sqrt{\mu}$ for $\sqrt{\mu}$; and this is indicated by writing $A'=S(A)$ (capital S). Further, A

[1] See Hilbert, *Bericht*, pp. 203 et seq., 277 et seq., and in particular Sommer's *Work*, p. 294, which I follow closely in the sequel.

and $S(A)$ are two numbers which are derived from each other by the substitution $-\sqrt{m}$ for $\sqrt{m}$.

It was seen in Vol. I, Art. 51 that

$$\Re(\sqrt{m};\ \sqrt{\mu}) = \Re(\tau),$$

where τ is a rational function of $\sqrt{m}$, $\sqrt{\mu}$, and where $\sqrt{\mu}$ is a rational function of τ, and also $\sqrt{m}$ is a rational function of τ. Such a function in fact is $\tau = \sqrt{m}+\sqrt{\mu}$, where τ satisfies an algebraic equation of the fourth degree with rational coefficients.

For

$$(\tau-\sqrt{\mu})^2 = m \quad \text{or} \quad \sqrt{\mu} = \frac{\tau^2-m+\mu}{2\tau}, \qquad \sqrt{m} = \frac{\tau^2-\mu+m}{2\tau},$$

and

$$(\tau^2-\mu-m)^2-4\mu m\tau^2 = 0.$$

Hence (Vol. I, Art. 44) all numbers of the realm $\Re(\sqrt{m};\ \sqrt{\mu})$ may be expressed rationally through τ in the form

$$A = a+a_1\tau+a_2\tau^2+a_3\tau^3,$$

where a, a_1, a_2, and a_3 are rational numbers. The number A satisfies an equation of the fourth degree with rational coefficients, namely (s being a substitution in $\mathfrak{k}$)

$$(x-A)[x-s(A)][x-S(A)][x-Ss(A)] = 0.$$

A number A of the relative realm $\Re(\sqrt{m};\ \sqrt{\mu})$ is said to be an integer, if it satisfies an equation

$$x^2+\alpha x+\beta = 0 = (x-A)[x-s(A)], \tag{1}$$

where α and β are integers of $\Re(\sqrt{m})$. Accordingly, such an integer A satisfies an equation of the fourth degree of the form

$$x^4+a_1x^3+a_2x^2+a_3x+a_4 = 0,$$

where a_1, a_2, a_3, and a_4 are rational integers.

From (1) it is seen that A is integral, if $A+S(A)$ and $AS(A)$ are integers of $\Re(\sqrt{m})$. The product $AS(A)$ of a number and its conjugate is called the *relative norm* of

the number A, and is denoted by $N_{\mathfrak{k}}(A)$, where with Hilbert $\mathfrak{k}$ is written for $\Re(\sqrt{m})$, while the realm $\Re(\sqrt{m};\ \sqrt{\mu})$ is denoted by $\mathfrak{K}$.

The relative norm of an integer of $\mathfrak{K}$ is an integer of $\mathfrak{k}$. If α is a number of $\mathfrak{k}$, its relative norm $N_{\mathfrak{k}}(\alpha)=\alpha^2$, since $S(\alpha)=\alpha$. From the definition just given for an integer, it is seen that an integer of $\mathfrak{K}$ which belongs to $\mathfrak{k}$, is an integer of $\mathfrak{k}$ and that an integer of $\mathfrak{K}$ which is rational, is also a rational integer.

The following theorem may be proved as in Vol. I, Art. 88:

THEOREM. *The sum, the difference, and the product of two integers of* $\mathfrak{K}$ *are integers of* $\mathfrak{K}$.

Accordingly, the difference

$$\Delta_{\mathfrak{k}}=A-S(A),$$

which is called the *relative different* of A, is integral if A is an integer. (Hilbert, *Math. Ann.*, Vol. 51, pp. 1 ff.)

Of particular importance is the conception of the *relative discriminant* of a number A, which is expressed through the formula

$$D_{\mathfrak{k}}(A)=\begin{vmatrix}1, & 1\\ A, & S(A)\end{vmatrix}^2=[A-S(A)]^2.$$

It may be shown that the relative discriminant of a number A is the negative relative norm of the relative different of A, that is

$$D_{\mathfrak{k}}(A)=-N_{\mathfrak{k}}(\Delta_{\mathfrak{k}}).$$

For observe that

$$A=\alpha+\beta\sqrt{\mu}, \qquad \Delta_{\mathfrak{k}}(A)=4\beta^2\mu, \qquad \text{and} \qquad N_{\mathfrak{k}}(\Delta_{\mathfrak{k}})=-4\beta^2\mu.$$

ART. **190. Basis of the Relative Realm.** Every number of the realm $\Re(\sqrt{m};\ \sqrt{\mu})=\mathfrak{K}$ may be written in the form

$$\frac{\alpha+\beta\sqrt{\mu}}{\gamma},$$

where α, β and γ are integers of $\mathfrak{k}$. It will be proved that there is an indefinite number of systems of four integers in $\mathfrak{K}$, such that every integer of $\mathfrak{K}$ may be expressed linearly through these four numbers with rational integral coefficients.

Observe that all the integers of $\mathfrak{K}$ fall into two categories

(1) integers that belong to $\mathfrak{K}$ and $\mathfrak{k}$;

(2) integers that belong to $\mathfrak{K}$ but *not* to $\mathfrak{k}$.

The first class may be expressed in the form $x+y\omega$, where x and y are rational integers and 1, ω form a basis of $\mathfrak{k}$. Accordingly we need consider further only the integers of the form

$$A=\frac{\alpha+\beta\sqrt{\mu}}{\gamma}, \qquad \text{where} \qquad \beta\neq 0.$$

Since

$$(x-A)[x-S(A)]=0=x^2+\frac{2\alpha}{\gamma}x+\frac{\alpha^2-\beta^2\mu}{\gamma^2}=0,$$

it is seen that $\frac{2\alpha}{\gamma}$ and $\frac{\alpha^2-\beta^2\mu}{\gamma^2}$ must be integral. In the expression for A we may assume that α, β, γ are free of ideal or rational factors. In the determination of the most general value for A as given below, observe that the prime factors of γ occur either to the second power in μ, or they must be divisors of 2.

Legendre denoted the greatest integer in $\frac{g}{2}$ by $\left[\frac{g}{2}\right]$; this integer may for brevity be denoted by $\bar{g}$.

For the realms $\mathfrak{R}(\sqrt{m})$, where $m\equiv 2$ or $m\equiv 3 \pmod 4$, the discriminant D is equal to $4m$, and consequently 2 contains ideal factors; on the other hand, if $m\equiv 1 \pmod 4$, $D=m$, it was shown that 2 is or is not factorable as a product of ideal factors according as $m\equiv 1 \pmod 8$ or $m\equiv 5 \pmod 8$ (see Vol. I, Art. 216, Case III).

THEOREM I. *Suppose that the stock-realm* $\Re(\sqrt{m})$ *contains only one class (the principal class,* $h=1$*) of ideals; and suppose that the prime factors of 2 are* λ_1, λ_2*, so that* $2=\lambda_1^{l_1}\lambda_2^{l_2}$*, where* $l_1+l_2\leqq 2$*,* l_1 *and* l_2 *being rational integers, of which one may be zero; further let* μ*, when distributed into its prime factors, be*

$$\mu=\lambda_1^{a_1}\lambda_2^{a_2}\pi_1^{e_1}\pi_2^{e_2}\cdots\pi_r^{e_r},$$

where at least of the rational numbers $a_1, a_2, e_1, e_2, \cdots, e_r$ *one must be odd (since* μ *is not a perfect square).*

Further, let $g_1\leqq l_1$ *and* $g_2\leqq l_2$ *be the greatest possible integers for which the congruence*

$$\mu\equiv\nu^2 \pmod{\lambda_1^{2(\sigma_1+\bar{a}_1)}\lambda_2^{2(\sigma_2+\bar{a}_2)}} \tag{1}$$

may be satisfied by an integer ν *of the realm* $\Re(\sqrt{m})$*. If* ν *is such a solution of the congruence (1) (see below) that*

$$\nu=\pi_1^{\bar{e}_1}\cdots\pi_r^{\bar{e}_r}\nu_1,$$

then is

$$\Omega=\frac{\nu+\sqrt{\mu}}{\lambda_1^{\sigma_1+\bar{a}_1}\lambda_2^{\sigma_2+\bar{a}_2}\pi_1^{\bar{e}_1}\cdots\pi_r^{\bar{e}_r}}=\frac{\nu+\sqrt{\mu}}{\gamma}$$

an integer of the realm $\Re(\sqrt{m};\ \sqrt{\mu})=\mathfrak{K}$*, and the four integers*

$$1,\ \omega,\ \Omega,\ \omega\Omega$$

form a basis of this realm. (Vol. I, Art. 98.)

Since μ is divisible by $\lambda_1^{a_1}\lambda_2^{a_2}$ it follows from (1) that ν is divisible by $\lambda_1^{\bar{a}_1}\lambda_2^{\bar{a}_2}$. Noting that $\pi_1^{\bar{e}_1}\cdots\pi_r^{\bar{e}_r}$ and $\lambda_1^{2(\sigma_1+\bar{a}_1)}\lambda_2^{2(\sigma_2+\bar{a}_2)}$ are relatively prime, it is seen that two integers ν_1 and σ_1 of the realm $\Re(\sqrt{m})$ may be found such that

$$\nu=\pi_1^{\bar{e}_1}\cdots\pi_r^{\bar{e}_r}\nu_1+\lambda_1^{2(\sigma_1+\bar{a}_1)}\lambda_2^{2(\sigma_2+\bar{a}_2)}\sigma_1;$$

or written as a congruence

$$\nu\equiv\pi_1^{\bar{e}_1}\cdots\pi_r^{\bar{e}_r}\nu_1 \pmod{\lambda_1^{2(\sigma_1+\bar{a}_1)}\lambda_2^{2(\sigma_2+\bar{a}_2)}}.$$

Hence under the assumption that $h=1$, every integer of

$\mathfrak{K}$ may be written in the form

$$\frac{\alpha+\beta\sqrt{\mu}}{\gamma},$$

where

$$\gamma=\lambda_1^{g_1+\bar{a}_1}\lambda_2^{g_2+\bar{a}_2}\pi_1^{\bar{c}_1}\cdots\pi_r^{\bar{c}_r},$$

and where α and β are integers of $\mathfrak{k}$. Finally observe that g_1 and g_2 may be greater than zero only when a_1 and a_2 respectively are even integers. If $g_1=0=g_2$ it is seen that $\nu=0$ and that Ω takes the simpler form $\Omega=\frac{\sqrt{\mu}}{\gamma}$.

ART. **191.** Suppose the number of classes h of the stock realm $\mathfrak{R}(\sqrt{m})$ is *greater* than unity, so that ideals take the place of algebraic integers in Theorem I. We accordingly have.

THEOREM II. *Under the assumption that $h>1$ let*

$$(2)=\mathfrak{l}_1\mathfrak{l}_2$$
$$(\mu)=\mathfrak{l}_1^{a_1}\mathfrak{l}_2^{a_2}\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r};$$

if further the congruence

$$\mu=\nu^2 \pmod{\mathfrak{l}_1^{2(g_1+\bar{a}_1)}\mathfrak{l}_2^{2(g_2+\bar{a}_2)}}$$

can be satisfied by an integer of the stock-realm $\mathfrak{R}(\sqrt{m})$ and if $\mathfrak{b}=(\beta_1,\beta_2)$ is an ideal, such that $\mathfrak{b}$ is relatively prime to $\mathfrak{l}_1$ and $\mathfrak{l}_2$ and such that

$$\mathfrak{l}_1^{g_1+\bar{a}_1}\mathfrak{l}_2^{g_2+\bar{a}_2}\mathfrak{p}_1^{\bar{c}_1}\cdots\mathfrak{p}_r^{\bar{c}_r}\mathfrak{b}=(\gamma),$$

where γ is a principal ideal, and if finally (ν) is so chosen (Art. 16) that

$$(\nu)=\mathfrak{p}_1^{\bar{c}_1}\cdots\mathfrak{p}_r^{\bar{c}_r}\mathfrak{n},$$

then $\Omega_1=\beta_1\frac{\nu+\sqrt{\mu}}{\gamma}$, $\Omega_2=\beta_2\frac{\nu+\sqrt{\mu}}{\gamma}$ are integers of $\mathfrak{K}$ (observe that β_1 and β_2 are each divisible by $\mathfrak{b}$) and the four integers

$$1,\ \omega,\ \Omega_1,\ \Omega_2$$

form a basis of the relative realm $\mathfrak{K}$. (Vol. I, Art. 296.)

The choice of γ in the denominator is in a measure arbitrary, according to the choice of $\mathfrak{b}$. However, every integer may be reduced to an integer having the special denominator γ. For suppose that

$$\Omega = \beta \frac{\sigma + \sqrt{\mu}}{\gamma_1},$$

where $\frac{\gamma}{\gamma_1} = \frac{\mathfrak{b}}{\mathfrak{b}_1}$. Multiplying the numerator and denominator of Ω by $\frac{\mathfrak{b}}{\mathfrak{b}_1}$, it is evident that

$$\Omega = \frac{\rho + \tau\sqrt{\mu}}{\gamma_1 \frac{\mathfrak{b}}{\mathfrak{b}_1}} = \frac{\rho + \tau\sqrt{\mu}}{\gamma},$$

since β by construction is divisible by $\mathfrak{b}_1$.

From any definite basis an indefinite number of quadruples of integers may be derived which form a basis of $\mathfrak{R}$. Any quadruple may be derived from an other quadruple through a substitution with integral coefficients of $\mathfrak{R}(\sqrt{m})$ and determinant equal to 1.

Finally it may be observed that an ideal $\mathfrak{b}$ may be so chosen that it contains as prime factors only the ideals $\mathfrak{l}_1$, $\mathfrak{l}_2$, $\mathfrak{p}_1 \cdots \mathfrak{p}_r$, so that therefore γ is a divisor of 4μ..

ART. **192. Ideals of the Relative Realm.** Observe that every ideal $\mathfrak{i} = (\iota, \iota_1)$ of the sub-realm $\mathfrak{k} = \mathfrak{R}(\sqrt{m})$ is also an ideal $\mathfrak{J}$ of the relative realm $\mathfrak{K} = \mathfrak{R}(\sqrt{m}; \sqrt{\mu})$, where the integers of $\mathfrak{i} = \mathfrak{J}$ are of the form $\iota\alpha + \iota_1\alpha_1$, in which α and α_1 go over all the integers of $\mathfrak{k}$. Reciprocally, an ideal $\mathfrak{J}$ of the relative realm $\mathfrak{K}$ is at the same time an ideal of $\mathfrak{k}$, if $\mathfrak{J}$ can be expressed through a system of integers, all of which belong to $\mathfrak{k}$. It is clear that not every ideal of $\mathfrak{K}$ is at the same time an ideal of $\mathfrak{k}$.

The definition of a principal ideal is the same as that given previously. (Art. 7.)

If the substitution $-\sqrt{\mu}\,||\,\sqrt{\mu}$ is made in all the integers of an ideal $\mathfrak{J}$, there results the relative conjugate ideal $\mathfrak{J}'$. An ideal $\mathfrak{J}$ which is equal to its relative conjugate ideal and which has no ideal of $\mathfrak{k}$ as a factor is called an *ambiguous* ideal of $\mathfrak{K}$.

If all the integers of an ideal are expressed through the basis 1, ω, Ω_1, Ω_2 and if the same methods are used as in Vol. I, Art. 206, it is seen that every ideal $\mathfrak{J}$ may be written in a form (i denoting a rational integer)

$$(i,\ \iota,\ I,\ I_1),$$

where i, ι, I, I_1 constitute a basis of the ideal. The definition of the product of two ideals and of the norm and the proof of the uniqueness of factorization of an ideal into its prime factors remain as in Art. 27.

If $n(\mathfrak{i}) = \mathfrak{i}\cdot\mathfrak{i}'$ denotes the norm of an ideal of $\mathfrak{k}$, and if $N(\mathfrak{i})$ denotes the norm of an ideal of $\mathfrak{K}$, it is seen that

$$N(\mathfrak{i}) = n(\mathfrak{i})^2.$$

If $\mathfrak{p}$ is an ideal of $\mathfrak{k}$, such that

$$\mathfrak{p} = \mathfrak{P}^2,$$

where $\mathfrak{P}$ is an ideal of $\mathfrak{K}$, it is evident that

$$n(\mathfrak{p})^2 = N(\mathfrak{p}) = N(\mathfrak{P}^2) = N(\mathfrak{P})^2$$

and that is

$$n(\mathfrak{p}) = N(\mathfrak{P}), \qquad \text{where} \qquad \mathfrak{p} = \mathfrak{P}^2.$$

An extension of this concept of the norm of an ideal is that of *the relative norm* of an ideal $\mathfrak{J}$, as denoted by the product

$$N_{\mathfrak{k}}(\mathfrak{J}) = \mathfrak{J}S(\mathfrak{J}) = \mathfrak{J}\cdot\mathfrak{J}'.$$

THEOREM. *The relative norm of an ideal $\mathfrak{J}$ of $\mathfrak{K}$ is an ideal of $\mathfrak{k}$.*

For if

$$\mathfrak{J} = (i,\ \iota,\ I,\ I_1),$$

then is

$$S(\mathfrak{J}) = (i,\ \iota,\ S(I),\ S(I_1))$$

and

$$\mathfrak{J}\cdot S(\mathfrak{J})=(i^2,\ i\iota,\ \iota^2,\ IS(I),\ I_1S(I_1),\ iI,\ IS(I_1),\ \cdots).$$

It may be proved as follows that all the elements of this latter ideal are integers of $\mathfrak{k}$. Denote I by $\alpha+\beta\sqrt{\mu}$ and I_1 by $\gamma+\partial\sqrt{\mu}$, and observe that

$$(\alpha+\beta\sqrt{\mu})(\gamma-\partial\sqrt{\mu})+(\alpha-\beta\sqrt{\mu})(\gamma+\partial\sqrt{\mu})=2(\alpha\gamma-\mu\beta\partial)$$

which is an integer of $\mathfrak{k}$, and that therefore $IS(I_1)+I_1S(I)$ is also an integer of $\mathfrak{k}$, as are $IS(I_1)$, $I_1S(I)$. Hence, $IS(I_1)$ and $I_1S(I)$ are also integers in $\mathfrak{k}$. For writing $IS(I_1)=\tau$, the above expressions are $\tau+S(\tau)$ and $\tau S(\tau)$, which are integers of $\mathfrak{k}$. Similarly it is seen that $iS(I)$ and iI are integers of $\mathfrak{k}$.

In particular it is seen that the square of an ambiguous ideal of $\mathfrak{K}$ is an ideal of $\mathfrak{k}$.

ART. **193.** For a better understanding of the relative realm, we may next introduce the concepts of the *relative different* and of the *relative discriminant* of $\mathfrak{K}$.

The first is by definition the greatest common divisor of the relative differences of all the integers of $\mathfrak{K}$ and is written

$$\mathfrak{D}_\mathfrak{k}=(A_1-S(A_1),\ A_2-S(A_2),\ \cdots);$$

while the relative-discriminant is

$$\mathfrak{d}=\mathfrak{D}_\mathfrak{k}^2=(A_1-S(A_1),\ A_2-S(A_2),\ \cdots)^2.$$

The relative different is an ideal of $\mathfrak{K}$, while the relative discriminant is an ideal of $\mathfrak{k}$, since $\mathfrak{D}_\mathfrak{k}=S(\mathfrak{D}_\mathfrak{k})$, so that $\mathfrak{d}$ is the square of an ambiguous ideal of $\mathfrak{K}$ or

$$\mathfrak{d}=N_\mathfrak{k}(\mathfrak{D}_\mathfrak{k}).$$

ART. **194.** THEOREM I. *If* $\mathfrak{p}$ *is a prime ideal of* $\mathfrak{k}$ *that is not a divisor of* (2), *but which enters* (μ) *to the eth power, then the relative discriminant of* $\mathfrak{K}$ *is divisible by* $\mathfrak{p}$ *to the first power when and only when e is an odd integer.*

THEOREM II. *If in* $\mathfrak{k}$ *there is a factorization of* (2) *such that* $(2) = \mathfrak{l}_1^{l_1}\mathfrak{l}_2^{l_2}$ *and if* $\mathfrak{l}_i$ *is a factor of* (μ) *to the* a_i *power, then the relative discriminant of* $\mathfrak{K}$ *is prime to* $\mathfrak{l}_i$, *when and only when there exists* [1] *in* $\mathfrak{k}$ *an integer* ν, *such that*

$$\mu \equiv \nu^2 \pmod{\mathfrak{l}_i^{2l_i+a_i}}.$$

Proof. The definitions of the relative discriminant as given in the preceding article, is expressed through the formula

$$\mathfrak{d} = (A_1 - S(A_1),\ A_2 - S(A_2),\ \cdots)^2;$$

and if the A's are expressed through the basal elements,

$$\mathfrak{d} = \left(\frac{2\beta_1\sqrt{\mu}}{\gamma},\ \frac{2\beta_2\sqrt{\mu}}{\gamma},\ \frac{2(x\beta_1+y\beta_2)\sqrt{\mu}}{\gamma},\ \cdots\right)^2.$$

It follows that

$$\mathfrak{d}(\gamma^2) = (\mu)(2)^2(\beta_1,\ \beta_2)^2 = (\mu)(2)^2\mathfrak{b}^2;$$

or, writing for μ, 2, their values of Art. 191,

$$\mathfrak{d} = \frac{\mathfrak{l}_1^{a_1}\mathfrak{l}_2^{a_2}\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}\mathfrak{l}_1^{2l_1}\mathfrak{l}_2^{2l_2}\mathfrak{b}^2}{\mathfrak{l}_1^{2\sigma_1+2\bar{a}_1}\mathfrak{l}_2^{2\sigma_2+2\bar{a}_2}\mathfrak{p}^{2\bar{e}_1}\cdots\mathfrak{p}_r^{2\bar{e}_r}\mathfrak{b}^2}.$$

For the proof of Theorem I, it is clear, if e_i is even and $\frac{e_i}{2} = \bar{e}_i$, that $\mathfrak{d}$ is prime to $\mathfrak{p}$; if, however, e_i is odd and $= 2\bar{e}_i + 1$, then $\mathfrak{d}$ contains as a factor $\mathfrak{p}$ to the first power. For Theorem II, observe that if

$$\mu \equiv \nu^2 \pmod{\mathfrak{l}_i^{2l_i+a_i}},$$

and if a_i is an even integer, we must put $g_i = l_i$ in the expression for γ. In this case the numerator and denominator of the expression for $\mathfrak{d}$ contain the factor $\mathfrak{l}_i^{2l_i+a_i}$ and $\mathfrak{d}$ is prime to $\mathfrak{l}_i$.

If, however, a_i is an odd integer, or if the congruence

$$\mu \equiv \nu^2 \pmod{\mathfrak{l}_i^{2(\sigma_i+\bar{a}_i)}}$$

exists only for $g_i < l_i$, then $\mathfrak{d}$ necessarily has the factor $\mathfrak{l}_i$.

[1] Hilbert, *Math. Ann.*, Vol. 51, pp. 5 ff.

With this is proved Theorem II. A combination of the above theorems gives rise to the following theorem:

THEOREM III. *If* (μ) *is prime to* (2), *and if the congruence*

$$\mu \equiv \nu^2 \pmod{2^2}$$

exists, the relative discriminant $\mathfrak{d}$ *of* $\mathfrak{K}$ *is prime to the ideal* (2).

ART. **195. The Prime Ideals of the Relative Realm.**

THEOREM I. *Let* $\mathfrak{p}$ *be a prime ideal of* $\mathfrak{k}$, *which is relatively prime to* (2) *and to* (μ). *Then in the realm* $\mathfrak{K}$, $\mathfrak{p}$ *is factorable as the product of two prime ideals* $\mathfrak{P}$ *and* $\mathfrak{P}'$, *if and only if* μ *is a quadratic residue with respect to* $\mathfrak{p}$, *that is, if an integer* α *in* $\mathfrak{k}$ *exists,*[1] *so that*

$$\alpha^2 \equiv \mu \pmod{\mathfrak{p}}.$$

Proof. If the congruence $\mu \equiv \alpha^2 \pmod{\mathfrak{p}}$ is satisfied; and if we put

$$\mathfrak{P} = (\mathfrak{p},\ \alpha + \sqrt{\mu}), \qquad \mathfrak{P}' = S(\mathfrak{P}) = (\mathfrak{p},\ \alpha - \sqrt{\mu}),$$

then $\mathfrak{P}$ is different from $\mathfrak{P}'$. For since $\mathfrak{p}$ and (μ) are relatively prime by hypothesis, it follows that α is also relatively prime to $\mathfrak{p}$, and therefore

$$(\mathfrak{p},\ \alpha + \sqrt{\mu},\ \alpha - \sqrt{\mu},\ 2\alpha,\ \cdots) = (1).$$

Further

$$\mathfrak{P}\mathfrak{P}' = (\mathfrak{p}^2,\ \mathfrak{p}(\alpha + \sqrt{\mu}),\ \mathfrak{p}(\alpha - \sqrt{\mu}),\ 2\mathfrak{p}\alpha,\ 2\mathfrak{p}\mu,\ \mathfrak{p}) = \mathfrak{p}.$$

With this, the first part of the theorem is proved. Reciprocally, suppose that in $\mathfrak{K}$ we have

$$\mathfrak{p} = \mathfrak{P}\mathfrak{P}_1.$$

Taking the relative norm of both sides of this equality, it follows that

$$\mathfrak{p}^2 = \mathfrak{P}S(\mathfrak{P})\mathfrak{P}_1 S(\mathfrak{P}_1);$$

and consequently $\mathfrak{P}_1 = S(\mathfrak{P})$, since the factorization of $\mathfrak{p}$ is a unique process.

[1] Hilbert, *Math. Ann.*, Vol. 51, pp. 8 ff.

If then A is any integer of $\mathfrak{B}$, which accordingly belongs to the relative realm $\mathfrak{R}$, we have

$$N_r(A) \equiv 0 \pmod{\mathfrak{p}}.$$

And, if $A = \frac{\alpha + \beta\sqrt{\mu}}{\gamma}$, it follows that

$$N_r(\alpha + \beta\sqrt{\mu}) \equiv 0 \pmod{\mathfrak{p}}.$$

First, suppose that (γ) is *not* divisible by $\mathfrak{p}$. If $\beta \equiv 0 \pmod{\mathfrak{p}}$, then we must also have $\alpha \equiv 0 \pmod{\mathfrak{p}}$, and in this case both α and β would be integers of the ideal $\mathfrak{p}$, and this case may be neglected.

If, however, β is prime to $\mathfrak{p}$, then (Art. 18) there exists an integer ξ of $\mathfrak{k}$ such that

$$\beta\xi \equiv 1 \pmod{\mathfrak{p}},$$

where ξ is also prime to $\mathfrak{p}$.

It follows from

$$\alpha^2 - \beta^2\mu \equiv 0 \pmod{\mathfrak{p}},$$

that also

$$(\alpha\xi)^2 - \mu \equiv 0 \pmod{\mathfrak{p}},$$

and accordingly μ is a quadratic residue with respect to $\mathfrak{p}$.

Were $\mathfrak{p}$ a divisor of γ, but not of β, there would be no change in the above result.

If, however, γ *is* divisible by $\mathfrak{p}^{e_1}$ and also α and β are divisible by $\mathfrak{p}^e$ where $e_1 \geqq e$, and were we to divide numerator and denominator of the expression for A by $\mathfrak{p}^e$, it is seen that α and β would be replaced by ideals. To avoid this, let $\mathfrak{i}$ be an ideal equivalent to and relatively prime to $\mathfrak{p}^e$ and put $\frac{\mathfrak{p}^e}{\mathfrak{i}} = \frac{\pi}{\sigma}$, where π is divisible by exactly the eth power of $\mathfrak{p}$ and where σ is an integer in $\mathfrak{k}$. We may write $\alpha = \frac{\pi}{\sigma}\alpha^*$ and $\beta = \frac{\pi}{\sigma}\beta^*$, where α^* and β^* are integers of

$\mathfrak{k}$ that are relatively prime to $\mathfrak{p}$. It follows as above that

$$\alpha^{*2}-\beta^{*2}\mu\equiv 0 \pmod{\mathfrak{p}}$$

in accord with the previous result.

In a similar manner for the prime ideal $\mathfrak{l}_i$, which is a factor of 2, the following theorem may be proved.

THEOREM II. *If $\mathfrak{l}_i (i=1, \text{ or } 2)$ is a prime ideal of $\mathfrak{k}$, whose l_i power is a divisor of 2, if, further, μ is prime to $\mathfrak{l}_i$ and is congruent to the square of an integer of $\mathfrak{k}$ with respect to $\mathfrak{l}_i^{2l_i}$, so that (Art. 194) the relative discriminant of $\mathfrak{K}$ is prime to $\mathfrak{l}_i$, then is $\mathfrak{l}_i$ factorable in $\mathfrak{K}$ into two prime ideals $\mathfrak{L}_i (i=1, 2)$ that are different from each other, if there is an integer α of $\mathfrak{k}$ such that*

$$\mu\equiv\alpha^2 \pmod{l_i^{2l_i+1}}.$$

ART. **196.** The two theorems of the preceding article offer a criterion as to whether or not prime ideals in $\mathfrak{k}$ which are not divisors of the relative discriminant, are factorable. The two Theorems III and IV that follow are generalizations of Theorems I and II.

THEOREM III. *The relative different of the relative realm $\mathfrak{K}$ is divisible by all and only those prime ideals of $\mathfrak{K}$ which are ambiguous.*

Proof. We saw that the relative different $\mathfrak{D}_t$ was an ideal in $\mathfrak{K}$ which was equal to its relative conjugate. It can at most be divisible by ambiguous prime ideals or through prime ideals of $\mathfrak{k}$. We shall see in Theorem IV below that the latter are the squares of ambiguous ideals of $\mathfrak{K}$.

For write

$$\mathfrak{D}_t=\mathfrak{P}\mathfrak{P}_1\cdots\mathfrak{P}_r,$$

where $\mathfrak{P}$, $\mathfrak{P}_1$, $\cdots$, $\mathfrak{P}_r$ are prime ideals in $\mathfrak{K}$. Since $\mathfrak{D}_t=S(\mathfrak{D}_t)$, we also have

$$\mathfrak{D}_t=S(\mathfrak{P})S(\mathfrak{P}_1)\cdots S(\mathfrak{P}_r).$$

Accordingly, either $\mathfrak{P}=S(\mathfrak{P})$ and is an ambiguous ideal, or

$\mathfrak{P}=S(\mathfrak{P}_i)$. If then two relative conjugate ideals $\mathfrak{P}_a$ and $S(\mathfrak{P}_a)$ are different, then $\mathfrak{D}_t$ is divisible by $\mathfrak{P}_a S(\mathfrak{P}_a)$. But $\mathfrak{P}_a S(\mathfrak{P}_a)(=\mathfrak{p}_a)$ is a prime ideal of $\mathfrak{k}$, including the ideals $\mathfrak{l}_i (i=1, 2)$. On the other hand we saw that

$$\mathfrak{d}=\mathfrak{D}_t^2=(A_1-S(A_1),\ A_2-S(A_2),\ \cdots)^2$$

has as factors, excepting the factors of 2, only those prime factors $\mathfrak{p}$ of the realm $\mathfrak{k}$ which enter μ to an odd power; and in this case $\mathfrak{p}$ enters $\mathfrak{d}$ only to the first power. If then $\mathfrak{D}_t$ contained $\mathfrak{p}$ as a factor, then $\mathfrak{d}(=\mathfrak{D}_t^2)$ must have $\mathfrak{p}$ as a factor at least to the second degree, which is *not* true.

Observe next that if $\mathfrak{d}$ contains as a factor the ideal which is a divisor of 2, it may be shown that $\mathfrak{l}_i=\mathfrak{L}_i S(\mathfrak{L}_i)$ where $\mathfrak{L}_i=S(\mathfrak{L}_i)$ is an ambiguous prime ideal of $\mathfrak{K}$.

For, if *first* $\mathfrak{l}_i$ enters as a factor to an odd power in μ, then the basal element Ω (see Art. 190) is of the form $\frac{\sqrt{\mu}}{\gamma}$ and clearly $\mathfrak{l}_i=\left(\mathfrak{l}_i, \frac{\beta}{\gamma}\sqrt{\mu}\right)^2=\mathfrak{L}_i^2$, where $\mathfrak{L}_i$ is an ambiguous ideal, different from (1), of $\mathfrak{K}$.

Suppose *secondly* that $\mathfrak{l}_i$ occurs to an even power a_i in μ, and that (Art. 191) the congruence

$$\mu\equiv\nu^2 \pmod{\mathfrak{l}_i^{2g_i+a_i}}$$

exists only for an integer $g_i<l_i$. It may be proved that integers α, β of $\mathfrak{k}$ exist such that

$$\mathfrak{l}_i=\left(\mathfrak{l}_i, \frac{\alpha+\beta\sqrt{\mu}}{\gamma}\right)\left(\mathfrak{l}_i, \frac{\alpha-\beta\sqrt{\mu}}{\gamma}\right)=\mathfrak{L}_i\mathfrak{L}_i',$$

where $\mathfrak{L}_i=\mathfrak{L}_i'$.

For it is possible under the given assumptions to determine an integer A of $\mathfrak{K}$, such that

$$A=\frac{\alpha+\beta\sqrt{\mu}}{\gamma},$$

where $N_t(A)$ is divisible by $\mathfrak{l}_i$. With this it will be

shown that $\mathfrak{l}_i$ is factorable as the square of an ambiguous ideal.

Due to the assumption regarding μ, it is clear that γ is divisible by $\mathfrak{l}_i^{g_i+a_i}$ and α is divisible by $l_i^{a_i}$. It remains only to show that

$$\alpha^2-\beta^2\mu\equiv 0 \pmod{\mathfrak{l}_i^{2g_i+a_i+1}}.$$

If, as in the proof of the first theorem of Art. 195, we write

$$\mu=\frac{\lambda^2}{\sigma^2}\mu^* \qquad \text{and} \qquad \alpha=\frac{\lambda}{\sigma}\alpha^*,$$

where λ is divisible by $\mathfrak{l}_i^{\frac{a_i}{2}}$ and no higher power of $\mathfrak{l}_i$, and σ is prime to $\mathfrak{l}_i$ while α^* and μ^* are also prime to $\mathfrak{l}_i$, then α^* and β may be determined so that

(i) $$\alpha^{*2}-\beta^2\mu^*\equiv 0 \pmod{\mathfrak{l}_i^{2g_i+1}}.$$

To prove this, observe that β being prime to $\mathfrak{l}_i$, this congruence may be written

(ii) $$\xi^2-\mu^*\equiv 0 \pmod{\mathfrak{l}_i^{2g_i+1}},$$

where the congruence of Art. 194, namely

$$\mu\equiv\nu^2 \pmod{\mathfrak{l}_i^{2(g_i+a_i)}},$$

becomes here

(iii) $$\mu^*\equiv\nu^{*2} \pmod{\mathfrak{l}_i^{2g_i}}.$$

There are two cases to be considered. If *first* the ideal (2) is a prime ideal in $\mathfrak{k}$, then since l_i is at most 1 and $g_i<l_i$, it follows that $g_i=0$. It remains to show that the congruence

$$\xi^2-\mu^*\equiv 0 \pmod 2$$

admits solution.

The integer 2 in $\Re(\sqrt{m})$ is prime only when $m\equiv 5 \pmod 8$ (see Vol. I, Art. 216). In this case the basis is 1, $\omega=\frac{1+\sqrt{m}}{2}$, where $\omega^2=\omega+\frac{m-1}{4}$.

Accordingly, we may write

$$\xi = x + y\omega, \qquad \mu^* = a + b\omega,$$

where x, y, a, b are rational integers. Since $\frac{m-1}{4} \equiv 1 \pmod 2$, it is seen that

$$\xi^2 - \mu^* \equiv x^2 + y^2 - a + (y^2 - b)\omega \equiv 0 \pmod 2,$$

a congruence which in all cases admits solution.

For $x^2 + y^2 - a \equiv 0 \pmod 2$ and $y^2 - b \equiv 0 \pmod 2$ may be simultaneously solved in rational integral values of x and y.

Suppose, *secondly*, that the integer 2 is factorable in the realm $\Re(\sqrt{m})$, so that either

$$(1^\circ)\ \ (2) = \mathfrak{l}_1\mathfrak{l}_2, \qquad \text{or} \qquad (2^\circ)\ \ (2) = \mathfrak{l}_1^2.$$

In the first case it remains to determine whether the congruence

(iv) $$\xi^2 - \mu^* \equiv 0 \pmod{\mathfrak{l}_i};$$

and in the second cases, whether the congruences

(v) $$\xi^2 - \mu^* \equiv 0 \pmod{\mathfrak{l}_1}, \qquad \text{when} \qquad g_1 = 0,$$

or

(vi) $$\xi^2 - \mu^* \equiv 0 \pmod{\mathfrak{l}_1^3}, \qquad \text{when} \qquad g_1 = 1$$

admit solution. It may be proved as follows that there exist solutions for each of these three possibilities. Take first the congruence (vi).

Observe that the congruence

$$\xi^2 - \mu^* \equiv 0 \pmod{\mathfrak{l}_1^2}$$

has a solution, since, due to the assumption

$$\mu \equiv \nu^2 \pmod{\mathfrak{l}_1^{2+a_1}},$$

it follows that

$$\mu^* \equiv \nu^{*2} \pmod{\mathfrak{l}_1^2},$$

and accordingly $\xi = \nu^*$.

Further, if $\xi = \nu^*$ is not a solution of (vi), put

$$\xi_1 = \xi + \lambda\kappa,$$

where λ is an integer of $\mathfrak{k}$ which is divisible by $\mathfrak{l}_1$ to the first power but by no higher power. The congruence (vi) is accordingly the same as

$$\frac{\xi^2-\mu^2}{2}+\kappa^2\frac{\lambda^2}{2}\equiv 0 \pmod{\mathfrak{l}_1};$$

and since $\frac{\lambda^2}{2}$ is prime to $\mathfrak{l}_1$ this congruence is of the same form as (iv); namely,

$$\xi^2-\mu^*\equiv 0 \pmod{\mathfrak{l}_1}.$$

Observe that for the congruences (iv) and (v) we have $n(\mathfrak{l}_1)=2$, n denoting the norm in the realm $\mathfrak{k}$; that is, all integers of $\mathfrak{k}$ with respect to the modulus $\mathfrak{l}_i$ may be distributed into two classes. It follows that every integer of $\mathfrak{k}$ is congruent, modulo $\mathfrak{l}_i$, to a rational integer which is prime to 2. Observe finally that the congruences

$$\xi^2-\mu\equiv 0 \pmod{\mathfrak{l}_i}$$

admit solution, since the congruence

$$x^2-a\equiv 0 \pmod{2}$$

may always be solved in integral values of x, whatever value the rational integer a may have.

With this it is proved that in all the cases above considered, the ideal $\mathfrak{l}_i$ may be factored in the realm $\mathfrak{K}$. Observe that

$$\frac{\alpha+\beta\sqrt{\mu}}{\gamma}+\frac{\alpha-\beta\sqrt{\mu}}{\gamma}\equiv 0 \pmod{\mathfrak{l}_i},$$

and

$$\frac{\alpha+\beta\sqrt{\mu}}{\gamma}-\frac{\alpha-\beta\sqrt{\mu}}{\gamma}\equiv 0 \pmod{\mathfrak{l}_i}.$$

It is seen that

$$\mathfrak{L}_i=\left(\mathfrak{l}_i,\frac{\alpha+\beta\sqrt{\mu}}{\gamma}\right)=\left(\mathfrak{l}_i,\frac{\alpha-\beta\sqrt{\mu}}{\gamma}\right)=\mathfrak{L}_i',$$

and thus it is proved that all ideals in question are

ambiguous; and accordingly the first part of our theorem is proved.

It remains to be proved that $\mathfrak{D}_r$ is divisible by all the ambiguous ideals of $\mathfrak{K}$. Let $\mathfrak{P}$ be an ambiguous ideal and

$$\mathfrak{p} = \mathfrak{P}^2.$$

Then, if n denotes the norm in $\mathfrak{k}$ and N the norm in $\mathfrak{K}$, we have (see Art. 192).

$$n(\mathfrak{p}) = n(\mathfrak{P}^2) = N(\mathfrak{P}).$$

From the equality of these two norms it is seen that the complete system of residues of the integers with respect to $\mathfrak{P}$ may be expressed through integers of $\mathfrak{k}$; that is, every integer of $\mathfrak{K}$ with respect to an ambiguous ideal $\mathfrak{P}$ is congruent to an integer of $\mathfrak{k}$. Observe that an integer that is *not* divisible by $\mathfrak{p}$ is *not* divisible by $\mathfrak{P}$.

From the congruence

$$A \equiv \alpha \pmod{\mathfrak{P}}$$

it follows that

$$S(A) \equiv \alpha \pmod{S(\mathfrak{P})}, \qquad \text{where} \qquad S(\mathfrak{P}) = \mathfrak{P};$$

and therefore

$$A - S(A) \equiv 0 \pmod{\mathfrak{P}}.$$

With this it is proved that *all* the integers of $\mathfrak{D}_r$ are divisible by $\mathfrak{P}$, and that is $\mathfrak{D}_r$ is divisible by $\mathfrak{P}$. With this Theorem III is proved.

THEOREM IV. *Every prime ideal of* $\mathfrak{k}$, *which is a divisor of the relative discriminant, is in the relative realm* $\mathfrak{K}$ *equal to the square of an ambiguous prime ideal. Reciprocally, every prime ideal* $\mathfrak{p}$ *of* $\mathfrak{k}$, *which is divisible by the square of a prime ideal of* $\mathfrak{K}$, *is a divisor of the relative discriminant* $\mathfrak{d}$.

Proof. If $\mathfrak{P}$ is a prime ideal of $\mathfrak{K}$, whose square is a prime ideal of $\mathfrak{k}$, then from above $\mathfrak{P}$ is a divisor of $\mathfrak{D}_r$, and consequently $\mathfrak{p}(=\mathfrak{P}^2)$ is a divisor of the relative discriminant, since $\mathfrak{d} = \mathfrak{D}_r^2$. And therefore every ideal of $\mathfrak{k}$,

which is equal to the square of an ambiguous ideal of $\mathfrak{R}$, is a divisor of $\mathfrak{d}$. If further $\mathfrak{p} = \mathfrak{P}^2\mathfrak{Q}$, then also

$$\mathfrak{p} = S(\mathfrak{P}^2)S(\mathfrak{Q}).$$

From this it follows that $\mathfrak{P} = S(\mathfrak{P})$ and $\mathfrak{Q} = S(\mathfrak{Q})$. Since $\mathfrak{P}S(\mathfrak{P})$ is an ideal in $\mathfrak{k}$ and is also a divisor of the prime ideal $\mathfrak{p}$ in $\mathfrak{k}$, it is seen that $Q = (1)$, so that $\mathfrak{p}$ is equal to the square of an ambiguous ideal. If further $\mathfrak{p}$ is a divisor of $\mathfrak{d}$, then is $\mathfrak{p}$ a divisor of $\mathfrak{D}_\mathfrak{k}^2$, and consequently $\mathfrak{p} = \mathfrak{P}^2$, since $D_\mathfrak{k}$ is divisible by all ambiguous ideals of $\mathfrak{R}$ and only by such ideals.

We may next follow Sommer and introduce numerical examples to illustrate certain more general phases of the theory that are due in a large measure to Hilbert. It will be seen that the theorems derived from the quadratic realms taken with respect to the realm of rational numbers as stock-realm have their analogues in the more general quadratic realms, where another quadratic realm is taken as stock-realm. In particular, the development and proof of the simplest law of reciprocity for prime integers and prime ideals of a stock-realm $\mathfrak{R}(\sqrt{m})$ are indicated by a consideration of the properties of such numbers and ideals in a more extended quadratic realm $\mathfrak{R}(\sqrt{m}; \sqrt{\mu})$.

ART. **197. The Relative Discriminant of an Upper Realm with Respect to a Stock-Realm in Which the Number of Classes Is Odd.** Hilbert (*Math. Ann.*, Vol. 51, p. 27) made the following assumptions and restrictions regarding the stock-realm $\mathfrak{k}$:

(1) *that it be an imaginary realm,*

(2) *that it have an odd number of classes.*

If the stock-realm is imaginary, it is evident that the relative realm in $\mathfrak{R}$ is also imaginary. This realm (see Art. 189) taken with respect to the realm of rational

numbers as the stock-realm is of the fourth degree, the four conjugate realms (including $\mathfrak{K}$) being imaginary.

It may be proved as in Vol. I, Art. 230 that in the realm $\mathfrak{K}=\mathfrak{R}(\sqrt{m};\ \sqrt{\mu})$ there exists *one* principal unit E differing from ± 1, whose norm is a unit in the stock-realm $\mathfrak{k}$, and therefore is ± 1. The realms $\mathfrak{R}(\sqrt{-1})$ and $\mathfrak{R}(\sqrt{-3})$ prove exceptions.

It was shown (see theorem of Vol. I, Art. 234) that the number of classes is *odd* under the assumptions above, only if $m\equiv 1 \pmod 4$ or if $m=-1$ or $m=-2$. (See Vol. I, Art. 216, III, and Art. 263.)

The law of reciprocity for the realm $\mathfrak{R}(\sqrt{-3})$ is treated by Dorrie in the thesis mentioned above, and the realm $\mathfrak{R}(\sqrt{-1})$ by Gauss (*Werke*, Vol. II, §§ 30 ff.). We may therefore exclude these two realms from the present discussion.

Accordingly, the realms to be considered here are the realms

$\mathfrak{R}(\sqrt{-2})$, $h=1$;	$\mathfrak{R}(\sqrt{-7})$, $h=1$;	$\mathfrak{R}(\sqrt{-11})$, $h=1$;
$\mathfrak{R}(\sqrt{-19})$, $h=1$;	$\mathfrak{R}(\sqrt{-23})$, $h=3$;	$\mathfrak{R}(\sqrt{-31})$, $h=3$;
$\mathfrak{R}(\sqrt{-43})$, $h=1$;	$\mathfrak{R}(\sqrt{-47})$, $h=5$;	etc.

ART. **198.** THEOREM. *If the stock-realm $\mathfrak{k}=\mathfrak{R}(\sqrt{m})$ is an imaginary realm in which h is an odd integer, then for every relative realm $\mathfrak{K}$ the relative discriminant $\mathfrak{d}$ with respect to $\mathfrak{k}$ is different from ± 1.*

Proof. It was seen in Art. 194 that the relative discriminant $\mathfrak{d}$ contained as a factor

(1) a prime ideal $\mathfrak{p}$, if μ is divisible by an odd power of $\mathfrak{p}$;

(2) the prime ideal $\mathfrak{l}$, if μ is divisible by $\mathfrak{l}^a$, while the ideal (2) is divisible by $\mathfrak{l}^l$, and if the congruence

$$\mu\equiv\alpha^2 \pmod{\mathfrak{l}^{2(l+\bar{a})}}$$

can *not* be satisfied by an integer α of $\mathfrak{k}$.

It was seen in Art. 196 that this congruence could be satisfied only if a was an even integer, say $a=2e$.

Suppose next that μ is divisible by the prime ideals $\mathfrak{p}_1$, $\mathfrak{p}_2, \cdots \mathfrak{l}$. Then it is clear that the relative discriminant $\mathfrak{d}$ can be prime to these factors, only if

$$(\mu)=\mathfrak{p}_1^{2e_1}\mathfrak{p}_2^{2e_2}\cdots\mathfrak{l}^{2e}.$$

Accordingly, we would have

$$(\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{l}^{e})^2=(\mu)\sim 1.$$

On the other hand we always have

$$(\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{l}^{e})^h\sim 1.$$

Since h is an odd integer by hypothesis, it follows that

$$(\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{l}^{e})\sim 1=(\nu)$$

say. It would therefore follow that $\mu=\epsilon\nu^2$, where ϵ is a unit and ν is an integer of $\mathfrak{k}$.

The realm $\Re(\sqrt{\epsilon\nu^2})$ is identical with the realm $\Re(\sqrt{\epsilon})$. And to prove that the relative discriminant is different from ± 1, it remains (see theorem at end of Art. 194) only to prove that in the stock-realm $\Re(\sqrt{m})$ the congruence $\epsilon=\alpha^2 \pmod 4$ cannot be solved. As the realms $\Re(\sqrt{-1})$ and $\Re(\sqrt{-3})$ have been excluded, the only value that the unit ϵ may have under the given assumptions is -1. It remains to see if the congruence

$$-1\equiv(x+y\omega)^2 \pmod 4$$

admits solution. Since

$$\omega=\frac{1+\sqrt{m}}{2}, \qquad \omega^2=\frac{m-1}{4}+\omega,$$

the above congruence is

$$-1\equiv x^2+\frac{m-1}{4}y^2+(2xy+y^2)\omega \pmod 4.$$

Accordingly, the two congruences

$$x^2+\frac{m-1}{4}y^2+1\equiv 0 \pmod 4,$$

and

$$2xy+y^2\equiv 0 \pmod 4$$

must be satisfied simultaneously.

From the second of these congruences it is seen that y must be an even integer and from the first it follows that

$$x^2+1\equiv 0 \pmod 4.$$

As this congruence can not be satisfied, it is seen that there does not exist a congruence of the form $\epsilon\equiv\alpha^2 \pmod 4$; and therefore the relative discriminant of $\mathfrak{R}(\sqrt{m};\sqrt{\epsilon})$ is *not* prime to 2.

Accordingly it is different from ± 1; and with this the theorem is proved.

ART. **199. Simple Cases of Hilbert's Quadratic Law of Reciprocity.** THEOREM I. *An integral or fractional number B of* $\mathfrak{K}$, *whose relative norm with respect to* $\mathfrak{k}$ *is* $+1$, *may be expressed as the quotient of two relative conjugate integers of the relative realm, and that is, in the form* $\frac{A}{S(A)}$, *where A is an integer of* $\mathfrak{K}$. (See Vol. I, Art. 234.)

Write $A_1=1+B$, where B is a number of $\mathfrak{K}$ that is different from -1. It follows that

$$S(A_1)=1+S(B)=\frac{1}{B}(1+B),$$

and therefore also $B=\frac{A_1}{S(A_1)}$. If a rational integer a is so chosen that aA_1 is integral, then is $aS(A_1)$ also integral. Hence writing $aA_1=A$, it follows that $B=\frac{A}{S(A)}$, where A is an integer in $\mathfrak{K}$.

The following is another interesting proof of the same theorem.

Let θ be an integer that determines the relative realm so that $\mathfrak{K}=\mathfrak{R}(\sqrt{m};\sqrt{m})=\mathfrak{R}(\theta)$. By hypothesis $BS(B)=+1$.

Further put

$$B_x=\frac{x+\theta}{x+S(\theta)}B,$$

and

$$A_x=1+B_x.$$

Observe that

$$B_xS(A_x)=B_x(1+S(B_x))=B_x+1=A_x$$

or

$$B_x=\frac{A_x}{S(A_x)}.$$

For x choose a rational integer a, such that $B_a\neq 0$; and put

$$A_1=\frac{A_a}{a+\theta}.$$

It is seen that

$$\frac{A_1}{S(A_1)}=\frac{a+S(\theta)}{a+\theta}\cdot\frac{A_a}{S(A_a)}=\frac{a+S(\theta)}{a+\theta}B_a=B.$$

Finally choose the rational integer b so that $bA_1=A$, where A is an integer of $\mathfrak{R}$. It follows that

$$B=\frac{A}{S(A)}$$

as above.

THEOREM. *If the relative discriminant of $\mathfrak{R}$ contains only the one prime ideal $\mathfrak{p}$ of $\mathfrak{k}$, then is the relative norm of the fundamental unit E of $\mathfrak{R}$ equal to -1.* (See Vol. I, Art. 235.)

Proof. Let E denote the fundamental unit of $\mathfrak{R}$. Were the relative norm of E equal to $+1$, it would follow from the preceding theorem that there existed an integer A of $\mathfrak{R}$ such that

$$E=\frac{A}{S(A)} \qquad \text{or} \qquad A=ES(A).$$

Hence every factor of A must also divide $S(A)$. This requires that A be divisible by ambiguous ideals or

ideals of $\mathfrak{k}$. By hypothesis $\mathfrak{P}$ is the only ambiguous ideal of $\mathfrak{R}$, where $\mathfrak{p} = \mathfrak{P}^2$. Observe further that in $\mathfrak{k}$ there exists an ideal $\mathfrak{m}$ such that

$$\mathfrak{m}\mathfrak{P} = \left(\frac{\beta\sqrt{\mu}}{\gamma}\right),$$

where μ and γ have the same meaning as in Art. 191. Further, since $+1$ and -1 are the only units of an imaginary realm, it follows that A must be of the form

$$A = \mathrm{H}\alpha \qquad \text{or} \qquad A = \mathrm{H}\xi\sqrt{\mu},$$

where α and ξ are numbers of $\mathfrak{k}$ and H a unit of $\mathfrak{R}$.

From this it would follow that

$$E = \frac{A}{S(A)} = \frac{\mathrm{H}}{S(\mathrm{H})} = \mathrm{H}^2,$$

and E accordingly would not be a fundamental unit. There remains then only the other possibility; namely,

$$N_{\mathfrak{k}}(E) = -1.$$

EXAMPLE. Exceptions have been made of the realms $\mathfrak{R}(\sqrt{-1})$ and $\mathfrak{R}(\sqrt{-3})$. Treat each case separately and make the required modifications.

ART. 200. From the theorem above it may be proved next that *the number of classes H of $\mathfrak{R}$ is odd.* (See Vol. I, Art. 235.)

Suppose that H were even. Then there would exist an ideal $\mathfrak{J}$, which was not a principal ideal, such that $\mathfrak{J}^2 \sim 1$. It would follow that $S(\mathfrak{J})^2 \sim 1$ and therefore also $(\mathfrak{J}S(\mathfrak{J}))^2 \sim 1$. On the other hand $\mathfrak{J}S(\mathfrak{J})(\sim \mathfrak{i})$ is an ideal in $\mathfrak{k}$. And since $\mathfrak{i}^h \sim 1$, where h is an odd integer, it would follow that $\mathfrak{J}S(\mathfrak{J}) \sim 1$. Then from $\mathfrak{J}^2 \sim 1$ and $\mathfrak{J}S(\mathfrak{J}) \sim 1$, we would have $\mathfrak{J} \sim S(\mathfrak{J})$, or $\mathfrak{J} = BS(\mathfrak{J})$, where B is a number in $\mathfrak{R}$, whose relative norm must be ± 1, since ± 1 are the only units of $\mathfrak{k}$.

If $N_r(B)=+1$, we have from the theorem of Art. 199, $B=\frac{S(A)}{A}$, where A is an integer of $\mathfrak{R}$. If, however, $N_r(B)=-1$, then is $N\mathfrak{f}(EB)=+1$, and we may write $EB=\frac{S(A)}{A}$. In either case the ideal equation $\mathfrak{J}=BS(\mathfrak{J})$ may be replaced by the other ideal equation $(A)\mathfrak{J}=S(A\mathfrak{J})$. Here again every ideal that divides $(A)\mathfrak{J}$ must be a factor of $S(A\mathfrak{J})$.

By hypothesis, there is only one ambiguous ideal of $\mathfrak{R}$, say $\mathfrak{P}$; and as above, $\mathfrak{P}$ being such that $\mathfrak{m}\mathfrak{P}=\left(\frac{\beta\sqrt{\mu}}{\gamma}\right)$, it follows that either $(A)\mathfrak{J}=\mathfrak{i}$ or $\mathfrak{m}(A)\mathfrak{J}=\mathfrak{i}\left(\frac{\beta\sqrt{\mu}}{\gamma}\right)$, where $\mathfrak{i}$ is an ideal of $\mathfrak{f}$. In either case $\mathfrak{J}$ would be equivalent to an ideal of $\mathfrak{f}$ or to a principal ideal. We would have on the one hand, $\mathfrak{J}^h\sim\mathfrak{i}^h\sim 1$, and on the other $\mathfrak{J}^2\sim 1$; and consequently $\mathfrak{J}\sim 1$, which is contrary to the assumption.

ART. **201.** Following a concept due to Gauss (*Works*, Vol. II, "Theoria resid. biquadrat.," Com. Sec. Nr. 36), Hilbert,[1] in his papers on the relative quadratic and relative Abelian realms, introduced for a convenient formulation of further theorems the *definition:*

A prime integer $\mathfrak{p}$ of $\mathfrak{f}$, that is not a factor of 2, with respect to which *every* unit of $\mathfrak{f}$ is a quadratic residue, is called *a primary prime ideal*, and every prime ideal which does not have this property is called a *non-primary* ideal.

Hence, in the present discussion, since the only units of $\mathfrak{f}$ are ± 1, it is clear that every prime ideal is primary if it is prime to 2, and with respect to which -1 is a quadratic residue. And for such primary prime ideals we have the following theorem:

[1] Hilbert, *Math. Ann.*, Vol. 51, pp. 48 ff.

THEOREM. *If* $\mathfrak{p}$ *is a primary prime ideal of* $\mathfrak{k}$, *there always exists in* $\mathfrak{k}$ *an integer* π, *such that* $(\pi)=\mathfrak{p}^h$ *and which has the further property that the congruence*

$$\pi \equiv \alpha^2 \pmod{4}$$

is satisfied through an integer α *of* $\mathfrak{k}$.

Proof. The ideal $\mathfrak{p}$ is, in a quadratic realm, either of the first or second degree. In the latter case, we have $\mathfrak{p}=(p)$ and since p is prime to 2, we have either

$$p \equiv 1 \pmod{4} \qquad \text{or} \qquad p \equiv -1 \pmod{4},$$

with which in this special case the theorem is proved. If, however, $\mathfrak{p}$ is a prime ideal of the first degree, so that $(p)=\mathfrak{p}\mathfrak{p}'$, then, due to the Fermat Theorem for every integer ρ of $\mathfrak{k}$ which is not divisible by $\mathfrak{p}$, there exists the congruence

$$\rho^{n(\mathfrak{p})-1} \equiv +1 \pmod{\mathfrak{p}}.$$

Hence in order that the congruence $\xi^2 \equiv -1 \pmod{\mathfrak{p}}$ be satisfied, as demanded in the hypothesis, we must have

$$(-1)^{\frac{n(\mathfrak{p})-1}{2}} \equiv +1 \pmod{\mathfrak{p}},$$

or

$$\frac{n(\mathfrak{p})-1}{2} \equiv 0 \pmod{2};$$

and that is, p must be of the form $4n+1$.

Writing

$$\mathfrak{p}^h = (a+b\omega),$$

where a and b are rational integers, and $\omega = \frac{1+\sqrt{m}}{2}$, we have

$$(p^h) = (a+b\omega)(a+b\omega')$$
$$= a^2+ab+b^2\frac{1-m}{4}.$$

Since $p \equiv 1 \pmod{4}$, it is clear that a and b cannot both

be even integers; and since further

$$a^2+ab+b^2\frac{1-m}{4}=\left(a+\frac{b}{2}\right)^2-\frac{m}{4}b^2,$$

which is a positive integer, since by hypothesis m is negative, there remains for a and b only the following possibilities:

(1) If $\frac{1-m}{4}\equiv 1 \pmod 4$, $a\equiv\pm 1$, $b\equiv 0$; or $a\equiv\pm 1$, $b\equiv\mp 1 \pmod 4$.

(2) If $\frac{1-m}{4}\equiv 2 \pmod 4$, then is $a\equiv\pm 1$, $b\equiv 0 \pmod 4$.

(3) If $\frac{1-m}{4}\equiv 3 \pmod 4$, we must have either $a\equiv\pm 1$, $b\equiv 0$; or $a\equiv 2$, $b\equiv\pm 1$; or $a\equiv\pm 1$, $b\equiv\pm 1 \pmod 4$.

(4) If $\frac{1-m}{4}\equiv 0 \pmod 4$, then necessarily $a\equiv\pm 1$, $b\equiv 0 \pmod 4$.

With regard to these possibilities it may be proved that one of the congruences

$$a+b\omega\equiv(x+y\omega)^2 \pmod 4,$$
$$-(a+b\omega)\equiv(x+y\omega)^2 \pmod 4,$$

may always be satisfied in rational integral values of x and y. And that is either the system

$$a-x^2+\frac{1-m}{4}y^2\equiv 0 \pmod 4,$$
$$b-2xy-y^2\equiv 0 \pmod 4;$$

or the system

$$-a-x^2+\frac{1-m}{4}y^2\equiv 0 \pmod 4,$$
$$-b-2xy-y^2\equiv 0 \pmod 4,$$

admits solution. With this the theorem is proved,

namely, that under the given assumptions, the congruence

$$\pi = \pm(a+b\omega) \equiv \alpha^2 \pmod{4}$$

may always be satisfied.

The reciprocal of this theorem is also true, namely:

THEOREM. *If π is an integer of $\mathfrak{k}$, for which the congruence $\pi \equiv \alpha^2$ (mod. 4) may be satisfied by an integer α of $\mathfrak{k}$, and, if (π) is the hth power of a prime ideal $\mathfrak{p}$ which does not divide 2, and that is $(\pi) = \mathfrak{p}^h$, then is $\mathfrak{p}$ a primary prime ideal, and that is, -1 is a quadratic residue of $\mathfrak{p}$.*

Proof. By hypothesis the relative discriminant of $\Re(\sqrt{m};\ \sqrt{\pi})$ contains the one prime factor $\mathfrak{p}$ and the relative norm of the fundamental unit E is equal to -1. Observe the form of the integers of $\Re(\sqrt{m};\ \sqrt{\pi})$ and put $E = \frac{\sigma+\rho\sqrt{\pi}}{2\tau}$, where ρ, σ, τ are integers of $\mathfrak{k} = \Re(\sqrt{m})$. It is seen that $\frac{2\sigma}{2\tau}$ is an integer, and that τ is at most divisible by $\mathfrak{p}^{\frac{h-1}{2}}$. From the relation

$$-1 = \frac{\sigma^2 - \rho^2\pi}{4\tau^2},$$

it is seen, since $\frac{\sigma}{\tau}$ and $\frac{\rho^2\pi}{\tau^2}$ are integers of $\mathfrak{k}$, that

$$-4 \equiv \lambda^2 \left(\text{mod. } \frac{\rho^2\pi}{\tau^2}\right),$$

and therefore also

$$-4 \equiv \lambda^2 \pmod{\mathfrak{p}}.$$

Since 2 is prime to $\mathfrak{p}$, an integer ξ of $\mathfrak{k}$ may be so chosen that $2\xi \equiv \pm 1 \pmod{\mathfrak{p}}$, and therefore finally

$$-1 \equiv \alpha^2 \pmod{\mathfrak{p}}.$$

The two theorems of the previous article lead at once to the following:

DEFINITION. If $\mathfrak{p}$ is a primary prime ideal of $\mathfrak{k}$ and if the integer π of $\mathfrak{k}$ in the equation $(\pi) = \mathfrak{p}^h$ be so chosen

as to sign that $\pi \equiv \alpha^2 \pmod 4$, then is π a *primary integer* of the primary ideal $\mathfrak{p}$. (Hilbert, *Bericht*, § 154.)

THEOREM. *If $\mathfrak{p}$ is a primary prime ideal of $\mathfrak{k}$ and if π is a primary integer of $\mathfrak{p}$, if $\mathfrak{r}$ is another prime ideal of $\mathfrak{k}$, and $\mathfrak{r}^h = (\rho)$, then it follows from $\left(\frac{\pi}{\mathfrak{r}}\right) = +1$ that $\left(\frac{\rho}{\mathfrak{p}}\right) = +1$.*

The notation $\left(\frac{\pi}{\mathfrak{r}}\right)$ is here again the extended Legendre Symbol. (Vol. I, Art. 216.)

Proof. Due to the hypothesis that $\left(\frac{\pi}{\mathfrak{r}}\right) = +1$, the prime ideal $\mathfrak{r}$ is factorable in $\mathfrak{R}(\sqrt{m};\ \sqrt{\pi}) = \mathfrak{R}$ as the product of two relative conjugate ideals

$$\mathfrak{r} = (\mathfrak{r}, A)(\mathfrak{r}, S(A)).$$

Since further π is a primary integer of $\mathfrak{p}$, the relative discriminant of $\mathfrak{R}$ contains only one prime factor $\mathfrak{p}$, and since H is an odd integer, there necessarily exists an odd rational integer, which is a divisor of H, say u, such that

$$\mathfrak{r}^u = (\Gamma)(S(\Gamma)),$$

where Γ and $S(\Gamma)$ are integers of $\mathfrak{R}$. This equation when raised to the h power may be written

$$(\rho)^u = (\Gamma_1)S(\Gamma_1);$$

and that is

$$\rho^u = \frac{\alpha+\beta\sqrt{\pi}}{2\gamma} \cdot \frac{\alpha-\beta\sqrt{\pi}}{2\gamma},$$

where α, β and γ are integers of $\mathfrak{k}$. Due to the properties of integers of the relative realm, the quantities $\frac{\alpha}{\gamma}$ and $\frac{\beta\sqrt{\pi}}{\gamma}$ are integers in it, and accordingly

$$4\rho^u \equiv \nu^2 \pmod{\mathfrak{p}}.$$

Next determine ξ so that

$$2\rho^{\frac{u-1}{2}}\xi \equiv 1 \pmod{\mathfrak{p}}.$$

It follows that

$$4\xi^2\rho^u \equiv \rho \equiv \xi^2\nu^2 \pmod{\mathfrak{p}},$$

or finally

$$\rho \equiv \alpha^2 \pmod{\mathfrak{p}}.$$

And this means that $\left(\frac{\rho}{\mathfrak{p}}\right) = +1$, as the theorem demands.

Through a repeated application of this theorem the following may be proved:

THEOREM. *If* $\mathfrak{p}$ *and* $\mathfrak{p}_1$ *are two primary prime ideals and* π *and* π_1 *are the corresponding primary integers, then always is*

$$\left(\frac{\pi}{\mathfrak{p}_1}\right) = \left(\frac{\pi_1}{\mathfrak{p}}\right).$$

Proof. From $\left(\frac{\pi}{\mathfrak{p}_1}\right) = +1$, it follows from the previous theorem that $\left(\frac{\pi_1}{\mathfrak{p}}\right) = +1$. Were $\left(\frac{\pi}{\mathfrak{p}_1}\right) = -1$, then also must $\left(\frac{\pi_1}{\mathfrak{p}}\right) = -1$. For if $\left(\frac{\pi_1}{\mathfrak{p}}\right) = +1$, then necessarily from the previous theorem $\left(\frac{\pi}{\mathfrak{p}_1}\right) = +1$ in contradiction to the assumption just made.

By means of the symbols for the norm-residues and the norm-non-residues, the general proofs of the law of reciprocity for the ideals and integers of a quadratic realm as stock-realm have been effected by Hilbert [1] in a manner analogous to the proofs given by him and as presented in Vol. I, Chapter X of the present treatise. The possibility of the proof under the assumptions stated in Art. 198 depends upon the fact that the number of classes of the relative realm is odd, and that all the classes of the relative realm belong to the same *genus*.

[1] Hilbert, *Math. Ann.*, Vol. 51, pp. 85 *et seq.*

The fact that the theorems here stated are true have lead to further endeavors in these directions and to better proofs of them with an extended treatment of the general theory. And the later development of this theory may eventually be of use in the establishment of other branches of mathematics, in particular the complex multiplication of elliptic functions.

The present work has to do with the *Foundations* of the General Theory; and it is pleasing to note that the recent developments and extensions of this theory are in the directions that are here indicated.

ART. **202. Examples for the Introduction of the Notion of Class-Realms.**[1] The following examples may serve by illustrating the theory to clarify the definitions which follow. The examples are found in Sommer's book, and are taken for the most part from the papers cited at the beginning of this chapter.

EXAMPLE 1. Let the stock-realm be $\Re(\sqrt{-5}) = \mathfrak{k}$ for which ± 1 are the only units. The number of classes is $h = 2$, and the basis is 1, $\omega = \sqrt{-5}$.

An interesting question is the following: *Are there any relative quadratic realms whose relative discriminant with respect to* $\mathfrak{k}$ *is* ± 1*?* Such a relative realm contains no ambiguous ideals and may be called an *unbranched* (unverzweigter) upper realm.

Since the number $\mu = -1$ of the realm $\mathfrak{k} = \Re(\sqrt{-5})$ contains no prime factor, and since the congruence

$$\mu = -1 \equiv \alpha^2 \pmod{4}$$

is satisfied by the integer $\alpha = \sqrt{-5}$ of $\mathfrak{k}$, the relative discriminant of $\Re(\sqrt{-5}; \sqrt{-1})(= \mathfrak{K})$ is prime to (2) and

[1] See Kronecker, *Werke*, Vol. 4, p. 118 and p. 126; and Hilbert, "Nachr. der kgl. Ges. d. Wissensch. zu Göttingen," *Math. phys. Klasse*, 1898, p. 370; and *Acta Math.*, Vol. 26, p. 99; and Hasse, *Math. Zeitschr.*, Vol. 31, p. 565. Numerous references are found in the *Report on Algebraic Numbers* by Dickson, Mitchell, Vandiver, and Wahlin, page 19.

contains no other prime factor. And that is, $\mathfrak{R}$ is a realm of the required kind.

A relative quadratic realm $\mathfrak{R}(\sqrt{m};\ \sqrt{\mu})$, *which with respect to a stock-realm* $\mathfrak{R}(\sqrt{m})$ *of class 2, has a relative discriminant* $=\pm 1$, *is called a* class-realm[1] *of the stock-realm.*

In the present example $\mathfrak{R}(\sqrt{-5};\ \sqrt{-1})$ is a class-realm of the quadratic stock-realm $\mathfrak{R}(\sqrt{-5})$. If we choose as a basis (Art. 190) of the class-realm the four integers $1,\ \omega=\sqrt{-5},\ \Omega=\dfrac{\sqrt{-5}+\sqrt{-1}}{2},\ \Omega_1=\sqrt{-5}\,\dfrac{\sqrt{-5}+\sqrt{-1}}{2}$, it is seen that Ω is also a unit, and that

$$\Omega S(\Omega)=\frac{-5+1}{4}=-1.$$

In the treatment of the factorization of the integers and ideals of the stock-realm each of the following statements typifies a definite fact, and characterizes a definite property of the class-realm.

(1) A prime integer p non-factorable in $\mathfrak{R}(\sqrt{-5})$, is factorable in $\mathfrak{R}(\sqrt{-5};\ \sqrt{-1})=\mathfrak{K}$ as the product of two prime ideals. For, note that the discriminant is $d=-20$, and that $\left(\dfrac{20}{p}\right)=\left(\dfrac{-5}{p}\right)$. Hence if $\left(\dfrac{-5}{p}\right)=-1$, then is either $\left(\dfrac{5}{p}\right)=1$, or $\left(\dfrac{-1}{p}\right)=1$. And therefore p is factorable in the realm $\mathfrak{R}(\sqrt{5})$ or in $\mathfrak{R}(\sqrt{-1})$. Further all numbers of these two realms are numbers of $\mathfrak{R}(\sqrt{-5};\ \sqrt{-1})$; and accordingly p is factorable in $\mathfrak{K}$.

For example $p=11$ is not factorable in $\mathfrak{R}(\sqrt{-5})$. Observe, however that $\left(\dfrac{5}{11}\right)=1$, and hence

$$(11)=(4+\sqrt{5})(4-\sqrt{5})=(9+2\Omega_1)(1-2\Omega_1).$$

[1] Hilbert, *Bericht*, pp. 278–279.

Similarly it is seen that $p=13,\ 17,\ 19,\ 31$ are not factorable in $\mathfrak{R}(\sqrt{-5})$. However in $\mathfrak{R}$ we have

$$(13)=(3+2\sqrt{-1})(3-2\sqrt{-1})=(3-2\omega+4\Omega)(3+2\omega-4\Omega),$$

$$(17)=(4+\sqrt{-1})(4-\sqrt{-1})=(4-\omega+2\Omega)(4+\omega-2\Omega),$$

$$(19)=\left(4+\frac{1+\sqrt{5}}{2}\right)\left(4+\frac{1-\sqrt{5}}{2}\right)=(7+\Omega_1)(2-\Omega_1),$$

$$(31)=(6+\sqrt{5})(6-\sqrt{5})=(11+2\Omega_1)(1-2\Omega_1).$$

(2) If p is a prime integer which is factorable in $\mathfrak{R}(\sqrt{-5})$ as the product of two ideals, there are the two cases to be considered:

(2a) $$p\equiv 1 \pmod 4,$$

or

(2b) $$p\equiv 3 \pmod 4.$$

(2a) In the first case the congruence

$$-1\equiv\alpha^2 \pmod{\mathfrak{p}}$$

may always be satisfied by an integer α of $\mathfrak{R}(\sqrt{-5})$. In fact, since $n(\mathfrak{p})=p$, every integer of $\mathfrak{R}(\sqrt{-5})$ is congruent, modulo $\mathfrak{p}$, to one of the rational integers $1, 2, \cdots, p$. As the congruence

$$-1\equiv x^2 \pmod{p}$$

admits solution, it follows that

$$-1\equiv\alpha^2 \pmod{\mathfrak{p}}$$

may be solved, as also the congruence

$$-1\equiv\alpha'^2 \pmod{\mathfrak{p}'}.$$

Accordingly, the ideals $\mathfrak{p}$ and $\mathfrak{p}'$ are further factorable in $\mathfrak{R}(\sqrt{-5};\sqrt{-1})$.

It may be proved that $\mathfrak{p}$ and $\mathfrak{p}'$ are principal ideals. For observe that the discriminant -20 of $\mathfrak{R}(\sqrt{-5})$ has as factors the two rational primes 2 and 5. The two classes, one being the principal class of the realm, therefore belong

to two different genuses. Observe, however, that both $\mathfrak{p}$ and $\mathfrak{p}'$ belong to the principal genus and therefore to the class of principal ideals. For we have

$$\left(\frac{-1}{p}\right)=+1, \quad \left(\frac{\pm 5}{p}\right)=+1, \quad \text{where} \quad p\equiv 1 \pmod 4.$$

(2*b*) The second case behaves differently. In this case the congruence

$$-1\equiv\alpha^2 \pmod{\mathfrak{p}}$$

does *not* admit solution. For since α must be congruent, modulo $\mathfrak{p}$, to a rational integer, we would have

$$-1\equiv x^2 \pmod p,$$

which can not be solved when $p=4n+3$.

Accordingly, the prime ideals $\mathfrak{p}$ of the second class (*i.e.*, the class other than the principal class) remain prime ideals in $\Re(\sqrt{-5};\ \sqrt{-1})$, and in this upper realm they are principal ideals, whereas they were not principal ideals of the stock-realm $\Re(\sqrt{-5})$. For observe that 2 is factorable in the realm $\Re(\sqrt{-1})$ in the form

$$2=(1+\sqrt{-1})(1-\sqrt{-1}).$$

Further write $\mathfrak{i}=(2,\ 1+\sqrt{-5})$ and denote by $\mathfrak{p}$ any ideal that is not a principal ideal of $\Re(\sqrt{-5})$. The prime divisors of the discriminant being 2 and 5, observe that

$$\left(\frac{2p,\ -5}{5}\right)=+1 \qquad \text{and} \qquad \left(\frac{2p,\ -5}{2}\right)=+1,$$

so that $\mathfrak{ip}$ is an ideal of the principal class, say $\mathfrak{ip}=(\alpha)$, where α is an integer of $\Re(\sqrt{-5})$. Hence $\mathfrak{i}^2\mathfrak{p}^2=(\alpha)^2$; and, since $h=2$, so that $\mathfrak{p}^2=(\pi)$, it follows that $\pm 2\pi=\alpha^2$ or $\pm 4\pi=\alpha^2\cdot 2$.

It follows in the relative realm $\Re(\sqrt{-5};\ \sqrt{-1})=\mathfrak{K}$ that

$$(\pi)=\frac{\alpha(1+\sqrt{-1})}{2}\cdot\frac{\alpha(1-\sqrt{-1})}{2}.$$

Observe that $\frac{\alpha(1+\sqrt{-1})}{2}$ and $\frac{\alpha(1-\sqrt{-1})}{2}$ are integers in $\mathfrak{R}$, since their sum and their product are integers. Further since $\mathfrak{p}$ is not factorable in $\mathfrak{R}$ and as the two integers $\frac{\alpha(1+\sqrt{-1})}{2}$ and $\frac{\alpha(1-\sqrt{-1})}{2}$ differ only by the factor $\sqrt{-1}$, it is seen that in the realm $\mathfrak{R}$ the ideal $\mathfrak{p}$ is $\frac{\alpha(1+\sqrt{-1})}{2}$. And that is, every prime ideal $\mathfrak{p}$ of the first degree of the realm $\Re(\sqrt{-5})$, which is not a principal ideal in this realm, is a principal ideal in $\mathfrak{R}$. The results of (1) and (2) taken together may be formulated in the theorem:

THEOREM. *Those prime ideals of the stock-realm* $\Re(\sqrt{-5})$, *which are principal ideals, are factorable in the class-realm* $\Re(\sqrt{-5};\sqrt{-1})$ *as the product of two ideals; on the other hand, those prime ideals in* $\Re(\sqrt{-5})$, *which are not principal ideals, remain prime ideals in the class-realm, becoming, however, principal ideals in this realm.*

The following examples will illustrate further the statement of this theorem:

$$(5)=(\sqrt{-5})^2$$

[*N.B.*, (5) is here an ideal],

$$(29)=(3+2\sqrt{-5})(3-2\sqrt{-5}),$$
$$(41)=(6+\sqrt{-5})(6-\sqrt{-5}),$$
$$(61)=(4+3\sqrt{-5})(4-3\sqrt{-5}).$$

Observe that $(\sqrt{-5})$, $(3+2\sqrt{-5})$, $(6+\sqrt{-5})$, $\cdots$ are principal ideals of $\Re(\sqrt{-5})$, which are factorable in the class-realm $\Re(\sqrt{-5};\sqrt{-1})$. For example

$$(\sqrt{-5})=(1+\Omega)(1+S(\Omega)),$$
$$(3+2\sqrt{-5})=(1-\sqrt{-5}+\sqrt{-1})(1-\sqrt{-5}-\sqrt{-1}),$$
$$(3-2\sqrt{-5})=(1+\sqrt{-5}+\sqrt{-1})(1+\sqrt{-5}-\sqrt{-1}),$$

$$(6+\sqrt{-5}) = \frac{5+\sqrt{-5}-(3-\sqrt{-5})\sqrt{-1}}{2} \times \frac{5+\sqrt{-5}+(3-\sqrt{-5})\sqrt{-1}}{2}$$
$$= (5+2\sqrt{-5}-3\Omega+\Omega_1) \times (5+2\sqrt{-5}-3S(\Omega)+S(\Omega_1));$$

and similarly

$$(4+3\sqrt{-5}) = (5+\Omega+\Omega_1)(5+S(\Omega)+S(\Omega_1)), \text{ etc.}$$

The following examples illustrate the behavior of the ideals in the class-realm which are not principal ideals in the stock-realm $\Re(\sqrt{-5})$. Observe that

$$(2, 1+\sqrt{-5}) = (1+\sqrt{-1}),$$

since

$$(2) = (1+\sqrt{-1})(1-\sqrt{-1}),$$

and

$$(1+\sqrt{-5}) = (1+\sqrt{-1})(-2+S(\Omega)-\Omega_1).$$

It is found also that

$$(3, 1+\sqrt{-5}) = (-2+S(\Omega)-\Omega_1),$$
$$(3, 1-\sqrt{-5}) = (3-\Omega+\Omega_1),$$
$$(7, 3+\sqrt{-5}) = (4+2\omega-3S(\Omega)+\Omega_1),$$
$$(23, 8+\sqrt{-5}) = (8+\omega+\Omega+3\Omega_1), \text{ etc.}$$

By factoring any given ideal into its prime factors, and applying the above processes to the prime factors, it is seen that what has been proved above for prime ideals is also true for ideals in general.

Finally, for the example of the stock-realm $\Re(\sqrt{-5})$, *it may be proved that the number of classes of the class-realm is* odd.

Assume that $\mathfrak{J}$ is an ideal of $\Re(\sqrt{-5}; \sqrt{-1})$, which is not a principal ideal. Note that $\mathfrak{J}^2 \sim 1$, since $\mathfrak{J}S(\mathfrak{J})$ is an

integer of $\Re(\sqrt{-5})$. It follows that

$$\mathfrak{J}^2 \sim \mathfrak{J}S(\mathfrak{J}) \qquad \text{or} \qquad \mathfrak{J} \sim S(\mathfrak{J}).$$

Accordingly, we may write $B = \dfrac{\mathfrak{J}}{S(\mathfrak{J})}$, and consequently

$$N_r(B) = \pm 1.$$

Were $N_r(B) = +1$, it follows as in Art. 199 that $B = \dfrac{(A)}{S(A)}$; and if $N_r(B) = -1$, since $N_r(E) = -1$, it is seen that

$$EB = \frac{(A)}{S(A)},$$

where A is an integer of the class-realm. In both cases $(A)\mathfrak{J} = S(A\mathfrak{J})$. It would therefore follow that $(A)\mathfrak{J}$ was an ideal of the stock-realm or the product of an ambiguous ideal of the class-realm by an ideal of the stock-realm. Since, however, the discriminant of the class-realm contains no prime ideal as a factor, and since there is no ambiguous ideal of the class-realm, it is seen that $(A\mathfrak{J})$ is an ideal of the stock-realm. Since h, the number of classes of $\Re(\sqrt{-5})$, is an odd integer and since $\mathfrak{J}^2 \sim 1$, it follows that $\mathfrak{J} \sim 1$. And that is, if the square of an ideal $\mathfrak{J}$ is a principal ideal, then $\mathfrak{J}$ also is itself a principal ideal.

If next we assume that the number of classes of the class-realm is even, say $H = 2^a n$, where n is an odd integer, then for every ideal of the class-realm it is seen that

$$\mathfrak{J}^{2^a n} \sim 1, \ \mathfrak{J}^{2^{a-1} n} \sim 1, \ \cdots, \ \mathfrak{J}^n \sim 1,$$

which being a contradiction to the assumption, shows that the number of classes is odd.

EXAMPLES

1. Following the method given for the realm $\Re(\sqrt{-5})$, prove that the same results may be derived for every stock-realm $\Re(\sqrt{m})$ with the number of classes equal to 2, where m is a negative prime

of the form $m \equiv 3 \pmod 4$. Show that the class-realms for such realms are $\Re(\sqrt{m};\ \sqrt{-1})$ and the fundamental unit ϵ of the realm $\Re(\sqrt{-m}) = \Re(\sqrt{m}\ \sqrt{-1})$ has as norm $n(\epsilon) = -1$ (Vol. I, Art. 230), which at the same time is a unit of $\Re(\sqrt{m};\ \sqrt{-1})$ with relative norm $= -1$.

2. Show that the theorems derived above for the realm $\Re(\sqrt{-5})$ are true for all imaginary stock-realms with class number 2. (Proved by Hilbert.)

ART. **203.** Under the assumptions that the stock-realm is imaginary and that $h = 2$, we may prove that the genus $g < 2$, where (Vol. I, Art. 262) $g = 2^{r-1}$ is the number of the different prime divisors of the discriminant of $\Re(\sqrt{m})$. If $m \equiv 1 \pmod 4$, and if $d = m$ is a rational prime integer, so that $r = 1$, then $g = 1$ and the class number is odd. For $h = 2$ there remains the further possibility that $g = 2$ and $r = 2$; and that is m is either a negative prime integer of the form $m \equiv 3 \pmod 4$ (see Vol. I, 263–264), the case treated above, or we may have two other cases, namely $m \equiv 2 \pmod 4$ or $m \equiv 1 \pmod 4$. In the first of these cases, the integer m is divisible by 2 and has a prime factor of the form $4n \pm 3$, and in the second case m is divisible by two primes the one of the form $p \equiv 1 \pmod 4$ and the other $q \equiv 3 \pmod 4$.

The following examples show that these possibilities actually occur. Note that Example 1 is found at the beginning of Art. 202 and that the following examples offer different phases of the subject.

EXAMPLE 2. The realm $\Re(\sqrt{-22})$ has the discriminant $d = -88$, $h = 2$, $g = 2$. If $\mathfrak{p}$ is any prime ideal that is not a divisor of 2 and is not a principal ideal, and if we put $(\pi) = \mathfrak{p}^2$, since $h = 2$, then the congruence $\pm\pi \equiv \alpha^2 \pmod 4$ may be satisfied by an integer for one or the other of the values $+\pi$ or $-\pi$. For if p is the rational prime that is divisible by $\mathfrak{p}$, and if we put $\pi = a + b\sqrt{-22}$,

then is $p^2=\pi\pi'=a^2+22b^2$. Since $p^2\equiv 1 \pmod 4$, it is seen that a must be odd and b even, so that the congruence

$$\pm(a+b\sqrt{-22})\equiv\alpha^2 \pmod 4$$

is satisfied by an integer α of $\Re(\sqrt{-22})$. If π_1 is written for that one of the integers $\pm\pi$, for which $\pi_1\equiv\alpha^2 \pmod 4$, it follows from the general theorems regarding relative realms, that the realm $\Re(\sqrt{-22};\ \sqrt{\pi_1})$ is one in which the relative discriminant contains no ideal that is different from ± 1. For example, let $\mathfrak{p}=(11,\ \sqrt{-22})$ so that $\mathfrak{p}^2=(11)$ and accordingly $\Re(\sqrt{-22};\ \sqrt{-11})$ is a class-realm of the stock-realm $\Re(\sqrt{-22})$, whose properties are set forth in the following four theorems:

THEOREM I. *The relative discriminant of the relative realm* $\Re(\sqrt{-22};\ \sqrt{-11})$ *with respect to the stock-realm* $\Re(\sqrt{-22})$ *is a unit.*

As a basis of the relative realm may be taken the four integers

$$1,\ \omega=\sqrt{-22},\ \Omega=11\cdot\frac{11+\sqrt{-11}}{22},\ \Omega_1=\sqrt{-22}\cdot\frac{11+\sqrt{-11}}{22}.$$

Since the relative realm contains all the integers of the two quadratic realms $\Re(\sqrt{-11})$ and $\Re(\sqrt{2})$, we have through a consideration of the character-system of the ideals the further theorem, namely:

THEOREM II. *Every principal prime ideal of the realm* $\Re(\sqrt{-22})$ *is factorable in the realm* $\Re(\sqrt{-22};\ \sqrt{-11})$ *as the product of two different relative conjugate prime ideals.*

The behavior of those ideals of $\Re(\sqrt{-22})$ that are not principal ideals, is indicated through the theorem:

THEOREM III. *The prime ideal of the stock-realm* $\Re(\sqrt{-22})$, *which are not principal ideals, remain ideals in* $\Re(\sqrt{-22};\ \sqrt{-11})$, *becoming, however, principal ideals.*

For it is seen that the ideal $(11,\ \sqrt{-22})$ becomes, in the relative realm, a principal ideal, since $(11,\ \sqrt{-22})$

$=(\sqrt{-11})$. If then $\mathfrak{p}$ is not a principal ideal, it is seen through a consideration of the character-system for such ideals that $\mathfrak{p}(11, \sqrt{-22}) = (\alpha)$, where (α) is an integer of the stock-realm; and consequently

$$(11)\mathfrak{p}^2 = \alpha^2, \qquad \text{or} \qquad \mathfrak{p}^2 = \frac{(\alpha)^2(\sqrt{-11})^2}{11^2}.$$

Since $\frac{\alpha\sqrt{-11}}{11}$ is an integer of the relative realm, it follows that $\mathfrak{p}$ is a principal ideal of it.

Due to the preceding theorems, we have finally the following:

THEOREM IV. *The class number of the relative realm* $\Re(\sqrt{-22}; \sqrt{-11})$ *is an odd integer.*

EXAMPLE 3. *The imaginary realm* $\Re(\sqrt{-15})$.

Here $-m = 5 \cdot 3$, where $5 \equiv 1 \pmod 4$ and $3 \equiv 3 \pmod 4$, $d = -15$, $h = 2$, and the genus g is 2, the basis being 1, $\omega = \frac{1+\sqrt{-15}}{2}$.

It is seen from the above considerations, that all those rational prime integers p, for which

$$\left(\frac{-15}{p}\right) = +1. \qquad \left(\frac{p}{3}\right) = +1, \qquad \left(\frac{p}{5}\right) = +1,$$

are factorable in the realm $\Re(\sqrt{-15})$ as the product of two principal ideals.

Let $\mathfrak{p}$ be any prime ideal that does not divide 2, and which is not a principal ideal. We may put $\mathfrak{p}^2 = (\pi)$ and prove that $\pm\pi \equiv \alpha^2 \pmod 4$.

Take for example either $\mathfrak{p} = (3, \sqrt{-15})$ or $\mathfrak{p} = (5, \sqrt{-15})$, and it is seen that, with respect to the stock-realm $\Re(\sqrt{-15})$, the relative realm $\Re(\sqrt{-15}; \sqrt{-3})$ or the relative realm $\Re(\sqrt{-15}; \sqrt{5})$ are class-realms having the same properties as were found in the preceding examples.

These examples offer an insight into the properties of the imaginary quadratic realms and of the quadratic relative realms. Especially noteworthy is the existence of a class-realm as a realm in which all the ideals of the stock-realm which are not principal ideals become principal ideals. (See Sommer, p. 328.)

ART. **204.** The behavior of the imaginary stock-realms is essentially different from that of the real stock-realms. For a real quadratic realm there exists the following definition introduced by Hilbert:

DEFINITION. A number of the real quadratic realm $\Re(\sqrt{m})$ is called *totally positive* [1] if α and its conjugate α' are both positive.

Further if α is a totally positive integer that is relative prime to 2 and if $\alpha \equiv \nu^2 \pmod 4$, where ν is an integer of $\Re(\sqrt{m})$, then is α a *primary number* of $\Re(\sqrt{m})$.

Hilbert introduced a more special definition of equivalence as follows:

DEFINITION. Two ideals $\mathfrak{i}$ and $\mathfrak{j}$ of the realm $\Re(\sqrt{m})$ are said to be equivalent in the *narrower* sense, if $\frac{\mathfrak{i}}{\mathfrak{j}} = \alpha$, where α is a totally positive number of $\Re(\sqrt{m})$. Any two ideals that are equivalent by this definition belong to the same class of ideals. The class-number in the narrower sense is denoted by $\bar{h}$.

Observe next that in the ideal equation $\frac{\mathfrak{i}}{\mathfrak{j}} = \alpha$, the number α is only determined as to a unit-factor. Hence in determining the class-number $\bar{h}$, it must be noted whether the norm of the fundamental unit is $+1$ or -1.

In fact, *first* let ϵ be the positive fundamental unit of $\Re(\sqrt{m})$ and suppose that $n(\epsilon) = -1$, so that ϵ' is

[1] See Dirichlet-Dedekind, 4th Edition, p. 578.

negative. Hence if α is assumed to be positive, then in all events one of the two numbers α or $\alpha\epsilon$ is totally positive. Accordingly, if in the wider sense the class-number is h, then also is $\bar{h}=h$.

Next, suppose that the fundamental unit ϵ is positive and that $n(\epsilon)=+1$. Hence also ϵ' is positive. The quotient α, which is defined through the equation $\frac{\mathfrak{i}}{\mathfrak{j}}=\alpha$, is, or is not, totally positive. In this case every class of the realm becomes in the narrower sense, two new classes. For if α_1 is a positive integer with a negative norm, then it follows from the equivalence of two ideals $\mathfrak{i}$ and $\mathfrak{j}$ in the wider sense the non-equivalence of the two ideals $\mathfrak{j}\asymp(\alpha_1)\mathfrak{i}$ in the restricted sense, although these ideals are equivalent in the wider sense. For example:

$$\begin{aligned}
&\Re(\sqrt{5});\quad \epsilon=\omega=\frac{1+\sqrt{5}}{2}, && n(\epsilon)=-1, && h=1, && \bar{h}=1,\\
&\Re(\sqrt{7});\quad \epsilon=8+3\sqrt{7}, && n(\epsilon)=1, && h=1, && \bar{h}=2,\\
&\Re(\sqrt{10});\ \epsilon=3+\sqrt{10}, && n(\epsilon)=-1, && h=2, && \bar{h}=2,\\
&\Re(\sqrt{15});\ \epsilon=4+\sqrt{15}, && n(\epsilon)=1, && h=2, && \bar{h}=4.
\end{aligned}$$

ART. **205.** It may be proved in general, that for a realm with *odd* class number $\bar{h}$ there can be no unbranched (Art. 202) relative realm, but on the other hand there are always such realms for all the other realms. For a realm with class-number $\bar{h}=2$ such a realm is at the same time a class-realm with the same properties as have been treated above for the class-realms of the imaginary stock-realm.

Consider next the special case $\Re(\sqrt{5})$ with the class number $h=1=\bar{h}$. If an unbranched relative realm existed for this stock-realm $\Re(\sqrt{5})$, and if such an upper realm was determined through μ, then μ can contain as factors only units or factors of 2. We have always

assumed that μ is free from quadratic factors. Since μ must be relatively prime to 2, it only remains to determine whether $\mu(=-1$ or $\pm\omega)$ offers an unbranched relative realm. In the latter case it must be determined whether the congruence $\pm\omega^2\equiv\alpha^2 \pmod 4$ may be satisfied by an integer α of $\Re(\sqrt{5})$. Writing $\alpha=x+y\omega$ and $\alpha^2=x^2+y^2+(2xy+y^2)\omega$, we have to determine whether the congruences

$$x^2+y^2\equiv 0 \pmod 4,$$
$$y^2+2xy\pm 1\equiv 0 \pmod 4,$$

may be solved simultaneously in integral values of x and y. In the latter congruence with the value -1, it is seen that y must be odd and x even. The first congruence in this case becomes

$$x^2+y^2\equiv y^2\equiv 0 \pmod 4.$$

Taking the value $+1$ in the second congruence, it is seen that both x and y must be odd, the first congruence becoming

$$x^2+y^2\equiv 2\not\equiv 0 \pmod 4.$$

Another proof, which is also applicable to the general case, is the following. Suppose for the fundamental unit ϵ one of the congruences $\pm\epsilon\equiv\alpha^2 \pmod 4$ were satisfied. It would follow that $\pm\epsilon'\equiv\alpha'^2 \pmod 4$ and consequently

$$\epsilon\epsilon'\equiv(\alpha\alpha')^2 \pmod 4 \qquad \text{or} \qquad -1\equiv(\alpha\alpha')^2 \pmod 4.$$

Since $\alpha\alpha'$ is a rational integer, this congruence does not admit solution. The realm $\Re(\sqrt{5};\ \sqrt{\pm\omega})$ is accordingly *not* an unbranched upper realm.

Further it may be proved that $\Re(\sqrt{5};\ \sqrt{-1})$ is not unbranched, since $-1\equiv\alpha^2 \pmod 4$ does *not* admit solution. And in general, since $n(\epsilon)$ must be -1, the value of m must be either $m\equiv 1 \pmod 4$ or $m\equiv 2 \pmod 4$. (Vol. I, Art. 240.) And the congruence $-1\equiv x^2 \pmod 4$ in either case does *not* admit solution for a

rational integer x. If on the other hand $\Re(\sqrt{m})$ is a realm with class number $h=1$, $\bar{h}=2$, whose fundamental unit has the norm $+1$, then there is always a class-realm. If $m\equiv 1 \pmod 4$ or $m\equiv 2 \pmod 4$, [the case $m\equiv 3 \pmod 4$ being considered below], write $\epsilon=\frac{\alpha}{\alpha'}$ (Vol. I, Art. 234), where we may write $\alpha=\frac{1+\epsilon}{t}$, t a rational integer, and α relative prime to 2. It follows that $\epsilon\alpha'^2=\alpha\alpha'$; and since $\alpha\alpha'$ is an odd rational integer, one of the congruences $\pm\alpha\alpha'\equiv 1 \pmod 4$ may always be satisfied. Hence there is a solution of the congruence $\pm\epsilon\alpha'^2\equiv\nu_1^2 \pmod 4$; and since α' is relative prime to 2, there is a solution of one or the other of the two congruences $\pm\epsilon\equiv\nu^2 \pmod 4$. And therefore also $\mu=\pm\epsilon$ determines an unbranched relative quadratic realm.

For the case $m\equiv 3 \pmod 4$, the number $\mu=-1$ determines such a realm. For we have immediately

$$-1\equiv(\sqrt{m})^2 \pmod 4.$$

ART. 206. EXAMPLE 4. Stock-realm $\Re(\sqrt{7})$. Observe that for this realm $h=1$, $\epsilon=8+3\sqrt{7}$, $N(\epsilon)=1$, and $\bar{h}=2$. In the narrower sense there are two classes of ideals:

1. To the principal class (or first class) belong the prime ideals $(3\pm\sqrt{7})$, (5), (11), (13), (17), (23), $(6\pm\sqrt{7})$, ...

2. To the class that is *not* a principal class, the second class, belong the prime ideals: $(3\pm 2\sqrt{7})$, $(9\pm 4\sqrt{7})$, $(4\pm 3\sqrt{7})$, ...

The prime ideals of the first class are either rational prime integers or exist through a factorization of the prime integer 2 or of rational primes p of the form $p\equiv 1 \pmod 4$. Observe that (Vol. I, Art. 249)

$$\left(\frac{p,\,7}{2}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{7-1}{2}}.$$

The prime ideals of the second class are $\mathfrak{p}$, where $\mathfrak{p}\mathfrak{p}' = p$ and $p \equiv 3 \pmod 4$. Observe that $-1 \equiv (\sqrt{7})^2 \pmod 4$, and accordingly that $\mu = -1$ determines an unbranched relative quadratic realm. If further $\mathfrak{p}$ is a prime ideal of the second class which is prime to 2, and if we put $(\pi) = \mathfrak{p}^2$ (since $\overline{h} = 2$), it may be proved that for one or the other of the values $\mu = \pm\pi$ there is always an unbranched relative realm.

Consider the realm $\Re(\sqrt{7}; \sqrt{-1}) = \mathfrak{R}$. The basal elements are

$$1,\ \omega = \sqrt{7},\ \Omega = \frac{\sqrt{7}+\sqrt{-1}}{2},\ \Omega_1 = \sqrt{7}\,\frac{\sqrt{7}+\sqrt{-1}}{2},$$

while $\epsilon = 8+3\sqrt{7}$ is a unit of $\Re(\sqrt{7})$. Note further that

$$E = \frac{(3+\sqrt{7})(1-\sqrt{-1})}{2}$$

is a unit of $\mathfrak{R}$, since $N(E) = \epsilon$.

With respect to every prime ideal of the first class there exists a congruence of the form $(-1) \equiv \alpha^2 \pmod{\mathfrak{p}}$, so that in $\mathfrak{R}$, these ideals are factorable into the product of two prime ideals. The above congruence can not be satisfied for prime ideals of the second class; and that is, when $p \equiv 3 \pmod 4$, the corresponding ideal factors $\mathfrak{p}$ not being reducible in $\mathfrak{R}$.

For example, for the ideals of the first class we have

$$(3+\sqrt{7}) = (1+\sqrt{-1})(5+2\omega-3\Omega-\Omega_1),$$
$$(5) = (2+\sqrt{-1})(2-\sqrt{-1}) = (2-\omega+2\Omega)(2+\omega-2\Omega),$$
$$(11) = (2+\sqrt{-7})(2-\sqrt{-7}) = (-5+2\Omega_1)(9-2\Omega_1),$$
$$(13) = (3+2\sqrt{-1})(3-2\sqrt{-1}),$$
$$(17) = (4+\sqrt{-1})(4-\sqrt{-1}),$$
$$(23) = (4+\sqrt{-7})(4-\sqrt{-7}),$$
$$(6+\sqrt{7}) = (3+2\omega-3\Omega-\Omega_1)(3+2\omega-3S(\Omega)-S(\Omega_1)).$$

The prime ideals of the second class remain prime ideals, becoming, however, ideals of the principal class.

For example

$$(3+2\sqrt{7}) = (3\sqrt{-1}+2\sqrt{-7}), \ \cdots.$$

EXAMPLES

1. Prove, as in the case of imaginary realms (Vol. I, Art. 234), that the class number, in the narrower sense, of $\Re(\sqrt{7};\ \sqrt{-1})$ is *odd*.

2. Prove that $\Re(\sqrt{-1})$ is a class-realm of $\Re(\sqrt{7})$.

3. In the realm $\Re(\sqrt{6})$, where $m=6\equiv 2 \pmod 4$, observe that $h=1, \epsilon=5-2\sqrt{6}, n(\epsilon)=+1, \bar{h}=2$. Prove that $\Re(\sqrt{6};\ \sqrt{-5-2\sqrt{6}}) = \Re(\sqrt{6};\ \sqrt{\epsilon})$ is a class-realm.

ART. **207.** EXAMPLE 5. $\Re(\sqrt{10})$. Observe that $h=\bar{h}=2$. Choose any prime ideal that is not a divisor of 2, and which does not belong to the principal class, for example

$$(3,\ 2+\sqrt{10}), \qquad (\pi)=\mathfrak{p}^2=(-1+\sqrt{10}).$$

The fundamental unit being $\epsilon=3+\sqrt{10}$, it follows from the theorem of Hilbert that $\pm\epsilon\pi\equiv\alpha^2 \pmod 4$ may be satisfied always by an integer α of $\Re(\sqrt{10})$. In fact, it is seen that

$$\mu=+\epsilon\pi=7+2\sqrt{10}\equiv(1+\sqrt{10})^2 \pmod 4.$$

Accordingly, $\Re(\sqrt{10};\sqrt{7+2\sqrt{10}}) = \mathfrak{K}$ is a relative quadratic unbranched realm.

As a basis of this realm may be chosen the integers

$$1,\ \omega=\sqrt{10},\ \Omega=\frac{3(1+\sqrt{10})+\sqrt{\mu}}{2},$$

$$\Omega_1=(2-\sqrt{10})\frac{3(1+\sqrt{10})+\sqrt{\mu}}{6}.$$

It is seen that

$$E=\frac{1+\sqrt{10}+\sqrt{\mu}}{2} \qquad \text{and} \qquad H=1+E$$

are units in $\mathfrak{K}$, since

$$N_t(E)=1, \qquad \text{and} \qquad N_t(H)=3+\sqrt{10}=\epsilon.$$

Note that, if we put

$$A = 20 - 4\omega + \Omega + 5\Omega_1,$$
$$B = 34 - 11\omega - 4\Omega - 10\Omega_1,$$
$$B_1 = 25 + 7\omega - 6\Omega + 4\Omega_1,$$
$$\Gamma = (3 - \sqrt{10})(B_1),$$

we have

$$(3) = (\sqrt{\mu})(A),$$
$$(2 + \sqrt{10}) = (\sqrt{\mu})(B);$$

and therefore

$$(3,\ 2 + \sqrt{10}) = (\mu),$$
$$(2,\ \sqrt{10}) = (B),$$
$$(2) = (B)^2,$$
$$(\sqrt{10}) = (B)(B_1),$$
$$(5) = (3 - \sqrt{10})^2 (B_1)^2 = (\Gamma)^2.$$

By means of the two equations

$$5 = \Gamma^2, \qquad \text{and} \qquad 2 = B^2,$$

we may offer numerous examples illustrating the laws of factoring in the relative realm.

Let (p) be a principal prime ideal of the stock-realm $\Re(\sqrt{10})$, such that $\left(\frac{10}{p}\right) = -1$. This equation is satisfied, if

(1) $$\left(\frac{2}{p}\right) = +1, \qquad \left(\frac{5}{p}\right) = -1,$$

or

(2) $$\left(\frac{2}{p}\right) = -1, \qquad \left(\frac{5}{p}\right) = +1.$$

This requires that one of the equations

$$p = x^2 - 2y^2,$$
$$p = x^2 - 5y^2,$$

admit solution in rational integral values of x and y.

And this means that in the relative realm

$$p = x^2 - 2y^2 = (x - By)(x + By),$$

or

$$p = x^2 - 5y^2 = (x - \Gamma y)(x + \Gamma y).$$

As examples we have

$$\begin{aligned}
7 &= 3^2 - 2\cdot 1^2 && \text{or} && (7) &= (3 - B)(3 + B),\\
11 &= 16 - 5 && \text{or} && (11) &= (4 - \Gamma)(4 + \Gamma),\\
17 &= 5^2 - 2\cdot 2^2 && \text{or} && (17) &= (5 - 2B)(5 + 2B),\\
19 &= 12^2 - 5\cdot 5^2 && \text{or} && (19) &= (12 - 5\Gamma)(12 + 5\Gamma),\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots
\end{aligned}$$

On the other hand if p is a prime integer that is factorable in $\mathfrak{R}(\sqrt{10})$, then is $\left(\frac{10}{p}\right) = 1$. There are accordingly the two possibilities

$$\text{(1)} \qquad \left(\frac{2}{p}\right) = 1, \qquad \left(\frac{5}{p}\right) = 1;$$

$$\text{(2)} \qquad \left(\frac{2}{p}\right) = -1, \qquad \left(\frac{5}{p}\right) = -1.$$

In the first case in the realm $\mathfrak{R}(\sqrt{10})$, p is factorable as the product of two principal ideals. For the realm $\mathfrak{R}(\sqrt{10})$ has two genuses, each with one class, and the factors of (p) belong to the principal genus. There exists accordingly an equation of the form

$$(p) = (x + \sqrt{10}y)(x - \sqrt{10}y).$$

Since, however, $p = x^2 - 2y^2$ and $p = x_1^2 - 5y_1^2$, it is seen that in the relative realm p is divisible by four different ideals. And each of the two principal ideals $x + \sqrt{10}y$, $x - \sqrt{10}y$ must be the product of two prime ideals of the relative-realm.

As examples, observe that the prime integers p, for which $\left(\frac{2}{p}\right) = 1$ and $\left(\frac{5}{p}\right) = 1$ are of the form $40n \pm 1$ and

$40n \pm 9$. It is seen that

$$31 = 11^2 - 10 \cdot 3^2 = (11 - 3\sqrt{10})(11 + 3\sqrt{10}) = \mathfrak{p}'\mathfrak{p},$$

$$\mu \equiv 4 \pmod{\mathfrak{p}'}, \qquad \mu \equiv 14^2 \pmod{\mathfrak{p}},$$

so that both $\mathfrak{p}'$ and $\mathfrak{p}$ are factorable in $\Re(\sqrt{10};\ \sqrt{\mu})$. Observe that

$$11 - 3\sqrt{10} = (3 - \sqrt{10})(2 - \sqrt{\mu})(2 + \sqrt{\mu});$$

and therefore as an ideal equation

$$(11 - 3\sqrt{10}) = (2 - \sqrt{\mu})(2 + \sqrt{\mu}),$$

while

$$(11 + 3\sqrt{10})$$

$$= \left(-1 + \sqrt{10} + 2\frac{(2-10)\sqrt{\mu}}{3}\right)\left(-1 + \sqrt{10} - 2\frac{(2-\sqrt{10})\sqrt{\mu}}{3}\right).$$

As another example it is seen that

$$41 = 9^2 - 10 \cdot 2^2 = (9 - 2\sqrt{10})(9 + 2\sqrt{10}) = \mathfrak{p}'\mathfrak{p},$$

and

$$\mu \equiv 4^2 \pmod{\mathfrak{p}'}, \qquad \mu \equiv 11^2 \pmod{\mathfrak{p}}.$$

It is clear that

$$(9 - 2\sqrt{10}) = (4 - \sqrt{\mu})(4 + \sqrt{\mu}),$$

$$(9 + 2\sqrt{10}) = \left(8 + 2\sqrt{10} + \frac{(5+2\sqrt{10})\sqrt{\mu}}{3}\right)$$

$$\times \left(8 + 2\sqrt{10} - \frac{(5+2\sqrt{10})\sqrt{\mu}}{3}\right).$$

As other examples, find the factors of 79, and 89.

For the second case where $\left(\frac{2}{p}\right) = -1$ and $\left(\frac{5}{p}\right) = -1$, the prime factors of (p) belong neither to the principal genus nor to the principal class, and accordingly are not principal ideals. Observe, however, that the equation

$$p = 2x^2 - 5y^2$$

always admits solution in rational integers x and y, so that

in the relative realm

$$(p) = (Bx + \Gamma y)(Bx - \Gamma y).$$

It was seen above that in the relative realm both $(2, \sqrt{10})$ and $(5, \sqrt{10})$ are principal ideals. For example,

$$\left(\frac{10}{13}\right) = 1, \qquad \left(\frac{2}{13}\right) = -1, \qquad \left(\frac{5}{13}\right) = -1,$$

and

$$(13) = (13, 6 - \sqrt{10})(13, 6 + \sqrt{10}) = \mathfrak{p}'\mathfrak{p}.$$

It is impossible to satisfy either one of the congruences

$$\mu \equiv \alpha_1^2 \pmod{\mathfrak{p}'} \qquad \text{or} \qquad \mu \equiv \alpha^2 \pmod{\mathfrak{p}}$$

through integers α_1 and α of $\Re(\sqrt{10})$. In fact, $\mu \equiv 8 \pmod{\mathfrak{p}}$ and $\mu \equiv 6 \pmod{\mathfrak{p}'}$; and that is, $\mathfrak{p}$ and $\mathfrak{p}'$ are *not* factorable in the relative realm.

In this realm, however, it may be proved that

$$(13, 6 + \sqrt{10}) = (3B + \Gamma),$$

and

$$(13, 6 - \sqrt{10}) = (3B - \Gamma).$$

EXAMPLES

1. Prove the analogous properties of (37).
2. Show that the class-number of $\Re(\sqrt{10}; \sqrt{7 + 2\sqrt{10}})$ is odd.

ART. **208.** It is proved, for example, by Hilbert (*Math. Ann.*, Vol. 51) that the theorems regarding the class-realms for quadratic stock-realms may be extended to the treatment of relative realms of the third and higher degrees. Take the stock-realm $\Re(\sqrt{-14})$ with class-number $h = 4$. As representatives of these classes are the ideals

$$(1), \ (2, \sqrt{-14}), \ (3, 1 - \sqrt{-14}), \ (3, 1 + \sqrt{-14}) = \mathfrak{i},$$

or

$$\mathfrak{i}, \ \mathfrak{i}^2, \ \mathfrak{i}^3, \ \mathfrak{i}^4 \sim 1 = (5 + 2\sqrt{-14}).$$

It is seen that

$$-5-2\sqrt{-14}\equiv(1+\sqrt{-14})^2 \pmod 4,$$

and that $\Re(\sqrt{-14};\ \sqrt{-5-2\sqrt{-14}})$ is an unbranched relative quadratic realm. As a basis of this realm we may choose the integers

$$1,\ \omega=\sqrt{-14},\ \Omega=9\,\frac{9(1+\sqrt{-14})+\sqrt{\mu}}{18},$$

$$\Omega_1=(2+\sqrt{-14})\,\frac{9(1+\sqrt{-14})+\sqrt{\mu}}{18}.$$

It may be proved that the ideals

$$\mathfrak{p}_2=(2,\ \sqrt{-14}),\quad \mathfrak{p}_3=\mathfrak{i}=(3,\ 1+\sqrt{-14}),\quad \mathfrak{i}'=(3,\ 1-\sqrt{-14})$$

are *not* factorable in the relative-realm.

The ideals

$$\mathfrak{p}_2=\mathfrak{P}_2=(12-3\sqrt{-14}+2\Omega_1) \qquad \text{and} \qquad \mathfrak{i}^2=(\sqrt{\mu})$$

are principal ideals, while $\mathfrak{i}$ and $\mathfrak{i}'$ are factorable in the relative-realm.

From this it is seen that the class-number for $\Re(\sqrt{-14};\ \sqrt{\mu})$, $\mu=-5-2\sqrt{-14}$, is still *even;* and it may be proved that with respect to a stock-realm $\Re(\sqrt{-14})$, a relative-realm of the fourth degree must be chosen in order to have a class-realm.

EXAMPLES

1. Extend the meaning of the Dedekind symbol $(\mathfrak{a},\ \mathfrak{b})$ to these relative-realms, and derive its properties.

2. Extend the Dedekind results as given in detail in Chapter VI to the relative realms. See Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, §§ 36–38.

CHAPTER XIII

THE GALOIS THEORY.[1] SUBSTITUTIONS. PERMUTATIONS

ART. **209. Primitive and Imprimitive Realms.** One of the principal problems of the present treatise is a study of realms of rationality by means of which the theory of algebraic numbers that arise from algebraic equations may be best developed and greatly simplified. And this in turn presents an arithmetical treatment of algebraic equations.

A system of numbers is defined (Vol. I, Art. 182) as a *realm of rationality* or a body of numbers, if such a body of numbers is so closed in itself that the four fundamental operations of addition, subtraction, multiplication and division, when performed with any number of the system, produce numbers which belong to the system. Such realms were extended in Vol. I, Chapts. II and III by the adjunction of algebraic numbers and functions of one or more variables, whose coefficients are rational or algebraic numbers. In particular, (Vol. I, Art. 49), if $\alpha, \beta, \gamma, \cdots$ are roots of the algebraic equations $A(x)=0$, $B(x)=0$, $C(x)=0, \cdots$, respectively, and if $\Re$ is the stock-realm, any quantity of the realm $\Re(\alpha, \beta, \gamma, \cdots)$ is an integral function in $\alpha, \beta, \gamma, \cdots$, whose coefficients belong to $\Re$, and (Vol. I, Art. 51) an algebraic quantity τ may be found such that $\Re(\alpha, \beta, \gamma, \cdots)=\Re(\tau)$. If τ satisfies an irreducible equation $f(x)=0$ of the nth degree, the realm $\Re(\tau)$ is said to be of the nth degree and any quantity σ

[1] See Galois, *Liouville's Journal*, Vol. XI (1846); Bachmann, *Math. Ann.*, Vol. 18; *Encykl. der math. Wiss.*, Vol. I, pp. 208 et seq.

of the realm $\Re(\tau)$ is of the form $\sigma = \chi(\tau)$, where $\chi(\tau)$ is an integral function in τ with coefficients that belong to the stock-realm. If the roots of $f(x) = 0$ are $\tau, \tau^{(1)}, \cdots, \tau^{(n-1)}$, the conjugate values of σ are

$$\sigma^{(1)} = \chi(\tau^{(1)}), \cdots, \sigma^{(n-1)} = \chi(\tau^{(n-1)}).$$

If the quantities $\sigma, \sigma^{(1)}, \cdots, \sigma^{(n-1)}$ are all different, σ is a *primitive* quantity of the realm $\Re(\tau)$; otherwise, it is *imprimitive.*

Forming the product

$$(x-\sigma)(x-\sigma^{(1)})\cdots(x-\sigma^{(n-1)}) = \Phi(x),$$

we saw (Vol. I, Art. 61) that $\Phi(x)$ is either irreducible or reducible. In the first case σ is a primitive quantity of $\Re(\tau)$; in the second case the quantity σ is the root of an irreducible equation $\varphi(x) = 0$ of degree n_1, say. It was seen (Vol. I, Art. 65) that

$$\Phi(x) = [\varphi(x)]^{n_2}, \qquad \text{where} \qquad n = n_1 \cdot n_2.$$

Accordingly, there exists the theorem:

THEOREM. *The function $\Phi(x)$ is either irreducible, or it is the power of an irreducible function. The n quantities that are conjugate with σ, where σ is any quantity of $\Re(\tau)$, and that is, the quantities $\sigma, \sigma^{(1)}, \cdots, \sigma^{(n-1)}$ are either all different from one another or they fall into n_1 systems where each σ occurs n_2 times. In the first case $\Phi(x)$ is irreducible, while in the second case $\Phi(x)$ is the n_2 power of an irreducible function of the n_1 degree.*

THEOREM. *Every quantity ω of the realm $\Re(\tau)$ may be expressed rationally in terms of any primitive quantity $\tilde{\omega}$ of $\Re(\tau)$.*

For, if

$$\Phi(x) = (x-\tilde{\omega})(x-\tilde{\omega}^{(1)})\cdots(x-\tilde{\omega}^{(n-1)}),$$

and if we put

$$\Phi(x)\left[\frac{\omega}{x-\tilde{\omega}} + \frac{\omega^{(1)}}{x-\tilde{\omega}^{(1)}} + \cdots + \frac{\omega^{(n-1)}}{x-\tilde{\omega}^{(n-1)}}\right] = \Psi(x),$$

where $\Psi(x)$ is an integral function of the $(n-1)$st degree in x, whose coefficients belong to $\mathfrak{R}$, it follows by writing $x=\tilde{\omega}$ that

$$\omega=\frac{\Psi(\tilde{\omega})}{\Phi'(\tilde{\omega})}.$$

We further see that any rational function of $\mathfrak{R}(\tau)$ is a rational function of $\tilde{\omega}$. Since $\tilde{\omega}$ is a rational function of τ, we have the equality of the realms $\mathfrak{R}(\tilde{\omega})=\mathfrak{R}(\tau)$.

THEOREM. *If $\tilde{\omega}$ is not a primitive quantity of $\mathfrak{R}(\tau)$, it is not possible to express every quantity of $\mathfrak{R}(\tau)$ rationally through $\tilde{\omega}$. The realm $\mathfrak{R}(\tilde{\omega})$ in this case is a divisor (Vol. I, Art. 65) of the realm $\mathfrak{R}(\tau)$ and the degree of $\mathfrak{R}(\tilde{\omega})$ is a divisor of the degree of $\mathfrak{R}(\tau)$.*

Proof. Every quantity in $\mathfrak{R}(\tilde{\omega})$ satisfies an equation in $\mathfrak{R}$ of degree n_1, say, where n_1 is a divisor of n and less than n. Hence a primitive quantity in $\mathfrak{R}(\tau)$, which satisfies an irreducible equation of the nth degree, cannot belong to $\mathfrak{R}(\tilde{\omega})$.

A realm $\mathfrak{R}(\tau)$ is called a *primitive* realm if besides the quantities of the stock-realm $\mathfrak{R}$ it contains no imprimitive quantities. It is clear that a realm whose degree is a prime number p, say, is necessarily primitive.

The following are important properties of realms:

If $\mathfrak{R}(\alpha)$ has a divisor $\mathfrak{R}(\beta)$, which is different from $\mathfrak{R}$, but which has $\mathfrak{R}$ as a divisor, so that β is a number of $\mathfrak{R}(\beta)$ but not of $\mathfrak{R}$, then $\mathfrak{R}(\beta)$ is an algebraic realm *over* (or above) $\mathfrak{R}$. Any quantity τ of $\mathfrak{R}(\beta)$ but not of $\mathfrak{R}$ determines a realm $\mathfrak{R}(\tau)$ which is a divisor of $\mathfrak{R}(\beta)$ and therefore also of $\mathfrak{R}(\alpha)$. The degree n_1 of $\mathfrak{R}(\tau)$ is a divisor of the degree n of $\mathfrak{R}(\alpha)$.

If τ, the quantity which determines the realm $\mathfrak{R}(\tau)$, does not determine the realm $\mathfrak{R}(\beta)$, and if γ is a quantity of $\mathfrak{R}(\beta)$ but not of $\mathfrak{R}(\tau)$, the realm $\mathfrak{R}(\tau, \gamma)$ is a realm that

divides $\Re(\beta)$. The degree of $\Re(\tau, \gamma)$ is greater than the degree of $\Re(\tau)$. Further if the degree of $\Re(\tau, \gamma)$ is not equal to $\Re(\beta)$, we can continue the process, forming the realms $\Re(\tau)$, $\Re(\tau, \gamma)$, $\cdots$, whose degrees continually increase and remain smaller than n until finally a realm is reached which is equal to $\Re(\alpha)$.

This gives rise to the following theorem regarding realms:

THEOREM. *Every divisor of* $\Re(\alpha)$, *which contains* $\Re$, *is an algebraic realm* $\Re(\tau)$, *say, over* $\Re$. *The degree of* $\Re(\tau)$ *is a divisor of the degree of* $\Re(\alpha)$, *and if both realms have the same degree, then they are identical.*

We may fashion the above definition in the terms below: *An algebraic realm over* $\Re$ *is primitive if besides itself and* $\Re$ *it has no other realm as divisor over* $\Re$.

ART. 210. **Normal Realms. The Galois Resolvent.** If $\Re(\alpha)$ is an algebraic realm, the conjugate realms

$$\Re(\alpha), \Re(\alpha'), \cdots, \Re(\alpha^{(n-1)})$$

are all of the same degree, and if one of them is contained in the other, these two realms are identical, since they are of the same degree.

A realm which is identical with all its conjugate realms is called a *normal* realm (Vol. I, Art. 53). In the normal realms the theorems are simpler. The great service rendered by Galois to algebra consists essentially in the fact that an arbitrary realm may be intimately associated with a normal realm and through a study of the normal realm, operations may be introduced which simplify the treatment of the quantities in the associated arbitrary realm.

If a realm of the mth degree $\Re(\rho)$ has the property that the quantities $\rho^{(1)}, \cdots, \rho^{(m-1)}$ which are conjugate to ρ are all contained in $\Re(\rho)$, then is $\Re(\rho)$ a normal realm.

For, in that case the realms $\mathfrak{R}(\rho^{(1)}), \cdots, \mathfrak{R}(\rho^{(m-1)})$ are all contained in $\mathfrak{R}(\rho)$ and therefore are identical with it.

An equation is called *a normal or Galois equation, if it is irreducible and has the property that all its roots may be expressed rationally (in $\mathfrak{R}$) in terms of a definite one of them.* In virtue of this definition, a primitive element of a normal realm of the mth degree is the root of a normal equation. Observe that the inverse of this is also true and that is, if ρ is the root of a normal equation through which the other roots may be rationally expressed, then $\mathfrak{R}(\rho)$ is a normal realm of the same degree as the equation. With this realm $\mathfrak{R}(\rho^{(1)})$, say, is conjugate and being a divisor of it and of the same degree is also identical with it. And with this we have the proof that in the case of a normal equation every root may not only be expressed rationally through a definite one of them but *it may also be expressed rationally through any one of them.*

With any realm it is possible and in the following manner to associate a Galois realm:

Let $F(x)=0$ be an arbitrary reducible or irreducible equation in $\mathfrak{R}$ of the nth degree, with the only restriction that it has no multiple roots.

Let the roots of this equation be $\alpha, \alpha^{(1)}, \cdots, \alpha^{(n-1)}$. The realm

$$\mathfrak{R}(\alpha, \alpha^{(1)}, \cdots, \alpha^{(n-1)}) = \mathfrak{N}$$

is called the *Galois realm* of the equation $F(x)=0$.

If $F(x)$ is irreducible, the realms $\mathfrak{R}(\alpha), \cdots, \mathfrak{R}(\alpha^{(n-1)})$ are all of the same degree as $F(x)$. In this case the realm $\mathfrak{N}$ is called the *norm* of each of the realms $\mathfrak{R}(\alpha)$, $\mathfrak{R}(\alpha^{(1)}), \cdots, \mathfrak{R}(\alpha^{(n-1)})$. If $\mathfrak{R}(\alpha)$ is a normal realm, it is identical with its norm.

In the general case it may be proved that $\mathfrak{N}$ is a normal realm, and that is, *the norm of an algebraic realm is a normal realm.* (See Vol. I, Art. 53.)

Another Proof. Let ρ be a primitive quantity of the realm

$$\mathfrak{N} = \mathfrak{R}(\alpha, \alpha^{(1)}, \cdots, \alpha^{(n-1)}),$$

so that

$$\mathfrak{N} = \mathfrak{R}(\rho);$$

and let m denote the degree of $\mathfrak{R}(\rho)$, so that ρ satisfies an irreducible equation of the mth degree, say,

$$g(t) = 0.$$

It remains to show that this is a Galois equation.

Since ρ is a quantity of the realm $\mathfrak{R}(\alpha, \alpha^{(1)}, \cdots, \alpha^{(n-1)})$, it is an integral function of its arguments, say,

$$\rho = \rho(\alpha, \alpha^{(1)}, \cdots, \alpha^{(n-1)}).$$

By permuting the α's in this function, it is seen that there are $\lfloor n - 1$ other functions that are thus produced. They are not all necessarily different. Denote these functions by $\rho, \rho_1, \rho_2, \cdots, \rho_{\lfloor n-1}$, and observe that, when one of the α's is interchanged with another, there is a change only in the sequence of the ρ's. This means that the product

$$(t-\rho)(t-\rho_1)\cdots(t-\rho_{\lfloor n-1}) = G(t),$$

is an integral function of the degree $\lfloor n$ in t, whose coefficients belong to $\mathfrak{R}$.

Observe that ρ satisfies the two equations $G(t) = 0$ and $g(t) = 0$. Since $g(t)$ is irreducible, it follows that $G(t)$ is divisible by $g(t)$, and that means that every root of $g(t)$ is a quantity in $\mathfrak{R}(\alpha, \alpha^{(1)}, \cdots, \alpha^{(n-1)})$.

Since

$$\mathfrak{R}(\alpha, \alpha^{(1)}, \cdots, \alpha^{(n-1)}) = \mathfrak{R}(\rho),$$

the meaning of the above is that every root of $g(t) = 0$ may be expressed rationally and in fact, integrally through ρ, thus proving that $g(t) = 0$ is a Galois equation.

Such an equation $g(t) = 0$ is called a *Galois resolvent* of the equation $F(x) = 0$.

A Galois resolvent may be defined through the following postulates:

An equation $g(t)=0$ is a Galois resolvent of a given equation $F(x)=0$ in $\Re$, if

(1) *$g(t)$ is irreducible; and if*

(2) *all of the roots of $F(x)=0$ are rationally expressible through one root of $g(t)$; and*

(3) *if a root ρ of $g(t)=0$ may be expressed rationally through the roots of $F(x)$.*

Further observe that *every Galois resolvent is a normal equation and that a normal equation is its own Galois resolvent.*[1]

ART. **211. The Substitutions of a Normal Realm.** Let $\Re(\rho)$ be a normal realm of the mth degree, where ρ is one of its primitive numbers. Further, let

$$g(t)=0 \tag{1}$$

be the irreducible equation of which ρ is a root, the other roots, the conjugates of ρ, being

$$\rho^{(1)}, \rho^{(2)}, \cdots, \rho^{(m-1)}. \tag{2}$$

By definition of a normal realm, it follows that

$$\rho^{(1)}=\Theta_1(\rho),\ \rho^{(2)}=\Theta_2(\rho),\ \cdots,\ \rho^{(m-1)}=\Theta_{m-1}(\rho), \tag{3}$$

where the Θ's are integral functions of at most the $m-1$ degree in their arguments. Observe that

$$g(\rho)=0, \qquad g[\Theta_k(\rho)]=0 \quad (k=1, 2, \cdots, m-1).$$

Since $\rho^{(1)}, \cdots, \rho^{(m-1)}$ are all roots of an irreducible equa-

[1] In this connection one may well read the historical remarks that are found in the preface to Camille Jordan's *Traité des substitutions*. I shall content myself with repeating here only one of his statements: "Ces beaux résultats (de Lagrange et d'Abel) n'étaient pourtant que le prélude d'une plus grand découverte. Il était réservé a Galois d'asseoir la théorie des equations sur sa base définitive, en montrant qu'à chaque équation correspond un groupe de substitutions, dans lequel se reflètent ses caractères essentiels, et notamment tous ceux qui ont trait à sa résolution par d'autres équations auxiliaires. D'après ce principe, étant donnée une équation quelconque, il suffira de connaître une de ses propriétés caractéristiques pour déterminer son groupe, d'ou l'on deduira réciproquement ses autres propriétés."

tion, it follows also that

$$g(\rho^{(h)})=0, \qquad g[\Theta_k(\rho^{(h)})]=0. \quad \begin{pmatrix} k=1, 2, \cdots, m-1 \\ h=1, 2, \cdots, m-1 \end{pmatrix}.$$

Thus it is evident that the quantities

$$\rho^{(h)}, \Theta_1(\rho^{(h)}), \cdots, \Theta_{m-1}(\rho^{(h)}) \tag{5}$$

are the roots of the equation $g(t)=0$; and are (neglecting the sequence) the same as the series of quantities

$$\rho, \Theta_1(\rho), \cdots, \Theta_{m-1}(\rho), \tag{6}$$

provided it is shown that no two of the quantities (5) are identical. If, however, say

$$\Theta_i(\rho^{(h)})=\Theta_k(\rho^{(h)}), \tag{7}$$

it would also follow that this relation was satisfied by the other roots of the irreducible equation (1), so that

$$\Theta_i(\rho)=\Theta_k(\rho). \tag{8}$$

And that is, $\rho^{(i)}=\rho^{(k)}$, which is not true, when $i \neq k$.

This gives rise to the following theorem:

THEOREM. *If ρ is changed into $\rho^{(h)}$, every one of the quantities that is conjugate with ρ becomes another definite one of these quantities, and no two different ones of these conjugate quantities are transposed into the same quantity.*

If in all functions of ρ, we write instead of ρ one of its conjugates, say, $\rho^{(a)}$, we make a *substitution*. These substitutions may be denoted by

$$\sigma_a=(\rho, \rho^{(a)}), \qquad (a=0, 1, 2, \cdots, m-1).$$

By σ_0 is to be understood the *identical* substitution (ρ, ρ), which is had when ρ is replaced by itself, and in virtue of which all quantities in $\Re(\rho)$ remain unchanged.

If upon any one of the roots (3), say,

$$\rho^{(h)}=\Theta_h(\rho),$$

the substitution σ_a is made, then $\rho^{(h)}$ becomes another root $\rho^{(k)}$ which is determined through

$$\rho^{(k)}=\Theta_h(\rho^{(a)})=\Theta_h\Theta_a(\rho)=\Theta_k(\rho). \tag{9}$$

Thus it is seen that $\rho^{(k)}$ is the same function of $\rho^{(a)}$ as $\rho^{(h)}$ is of ρ. It is evident that

$$\sigma_a = (\rho^{(h)}, \rho^{(k)}) = [\rho^{(h)}, \Theta_h \Theta_a(\rho)]$$

on the one hand, while from above $\sigma_a = (\rho, \rho^{(a)})$.

In this presentation $\rho^{(h)}$ was an arbitrary root of (3) and the corresponding $\rho^{(k)}$ is determined through (9). It is evident also that with a given σ_a the quantity $\rho^{(k)}$ may be arbitrarily chosen and the corresponding $\rho^{(h)}$ found. It is only necessary in the expression $\Theta_h(\rho^{(a)})$ to let h go through the values $0, 1, \cdots, m-1$, since in the doing of it, each root $\rho^{(k)}$ of $g(t) = 0$ occurs once and only once.

With this is proved the theorem:

THEOREM. *Every substitution σ_a may be expressed in the form $(\rho^{(h)}, \rho^{(k)})$, where either $\rho^{(h)}$ or $\rho^{(k)}$ is an arbitrary one of the roots (3), while the other root is completely determined through σ_a.*

Hence the number of different substitutions, including the identical substitution, is m, the degree of the realm $\Re(\rho)$. Each of these substitutions has the property of transforming the complex of numbers of $\Re(\rho)$ into the same complex. The numbers, of course, follow a different sequence, each number becoming another definite number and no two different numbers being transformed into the same numbers due to formulas (7) and (8).

The operations

$$\sigma_a = (\rho, \rho^{(a)}) \qquad (a = 0, 1, \cdots, m-1)$$

are therefore called the *substitutions* of the realm $\Re(\rho)$.

If $\omega = \varphi(\rho)$ is a quantity of $\Re(\rho)$, which remains unchanged when ρ is replaced by $\rho^{(a)}$; and that is, if $\varphi(\rho) = \varphi(\rho^{(a)})$, we say that the quantity ω *permits* the substitution $(\rho, \rho^{(a)})$ or σ_a. The quantities ω which permit no other substitution than the identical substitution, are the primitive elements of the realm $\Re(\rho)$. A quantity which

permits all substitutions σ_a is necessarily a quantity of $\mathfrak{R}$. For, if

$$\tau = \tau^{(1)} = \tau^{(2)} = \cdots = \tau^{(m-1)},$$

it follows that

$$\tau = \frac{\tau + \tau^{(1)} + \cdots + \tau^{(m-1)}}{m},$$

which is a quantity of the stock-realm.

ART. **212. Composition of Substitutions.** If in any function of the root ρ, the quantity ρ is first replaced by $\rho^{(a)}$ and then $\rho^{(a)}$ by $\rho^{(b)}$, the result is the same as if ρ had at once been replaced by $\rho^{(b)}$. Accordingly, if we put

(1) $\sigma = (\rho, \rho^{(a)}), \qquad \sigma' = (\rho^{(a)}, \rho^{(b)}), \qquad \sigma'' = (\rho, \rho^{(b)}),$

it is immaterial whether the substitution σ and then the substitution σ' are made, or whether σ'' is at once made. We may therefore say that σ'' is *compounded* of σ and σ'. This relation is symbolically denoted by the expression

$$\sigma\sigma' = \sigma''.$$

It was seen in the preceding article that in the notation of the substitution $(\rho^{(h)}, \rho^{(k)})$ either $\rho^{(h)}$ or $\rho^{(k)}$ may be arbitrarily chosen. Hence, in the above substitutions it is possible to choose $\rho^{(a)}$ and $\rho^{(b)}$ such that σ and σ' are two substitutions arbitrarily fixed among the m substitutions of the realm $\mathfrak{R}(\rho)$, while therefrom σ'' is completely determined. Similarly, if σ and σ'' are given, then is σ' uniquely determined. For, if ρ is arbitrarily chosen, then $\rho^{(a)}$ is determined through σ while $\rho^{(b)}$ is found through σ'', and with this $\sigma' = (\rho^{(a)}, \rho^{(b)})$ is fixed.

It is thus seen that if among the substitutions of a fixed normal realm $\mathfrak{R}(\rho)$, any two are arbitrarily chosen, and if the relation

$$\sigma\sigma' = \sigma''$$

exists, then the third substitution is thereby uniquely determined. In this symbolic multiplication of substi-

tutions it is evident that the commutative law does not in general hold, as evidently

$$\sigma\sigma' \neq \sigma'\sigma.$$

The associative principle is, however, applicable. This gives rise to the theorem:

THEOREM. *If σ, σ' and σ'' are any substitutions of the realm $\Re(\rho)$, then is*

$$(\sigma\sigma')\sigma'' = \sigma(\sigma'\sigma'').$$

For, from the preceding article $\rho^{(a)}$, $\rho^{(b)}$, $\rho^{(c)}$ may be so determined that

$$\sigma = (\rho, \rho^{(a)}), \qquad \sigma' = (\rho^{(a)}, \rho^{(b)}), \qquad \sigma'' = (\rho^{(b)}, \rho^{(c)});$$

and then it follows that

$$\sigma\sigma' = (\rho, \rho^{(b)}), \qquad (\sigma\sigma')\sigma'' = (\rho, \rho^{(c)}),$$
$$\sigma'\sigma'' = (\rho^{(a)}, \rho^{(c)}), \qquad \sigma(\sigma'\sigma'') = (\rho, \rho^{(c)}).$$

Hence the substitution that is compounded of the three substitutions σ, σ', σ'' is denoted briefly by $\sigma\sigma'\sigma''$; and in general, the substitution that is compounded of any number of components σ, σ', $\sigma'' \cdots$ is $\sigma\sigma'\sigma'' \cdots$. For the quantities $\rho^{(a)}$, $\rho^{(b)}$, $\rho^{(c)}$, $\rho^{(d)}$, $\cdots$ may be always so determined for any substitutions σ, σ', σ'', σ''', $\cdots$ that

$$(\rho, \rho^{(a)})(\rho^{(a)}, \rho^{(b)})(\rho^{(b)}, \rho^{(c)})(\rho^{(c)}, \rho^{(d)}) = (\rho, \rho^{(d)}).$$

And this evidently may be extended to any number of components.

In view of the properties[1] that have been developed in this article, we may call the m substitutions of the normal realm $\Re(\rho)$ a *group;* and in fact, a *finite group of degree m.* Such a group is known as the *substitution group* of the realm $\Re(\rho)$.

[1] For an account of Galois's works see *Journ. de math.*, 11, pp. 381–444; or his *Oeuvres* published in 1897. In this connection, the reader should consult L. E. Dickson's *Modern Algebraic Theories*, published 1926 by Sanborn and Co. For sources on Galois's life, see *Bulletin of the Amer. Math. Soc.*, Vol. 4, 1897–99, pp. 332 et seq.; *Scientific Monthly*, 1921, pp. 363–375.

ART. 213. **Permutation Groups.**[1] In Art. 210 it was seen that with any equation

$$F(x)=0, \tag{1}$$

in which there were no double roots, there was associated a normal realm $\Re(\rho)$. The roots of (1) all belong to this realm. If the roots of (1) are denoted by

$$\alpha,\ \alpha^{(1)},\ \cdots,\ \alpha^{(n-1)}, \tag{2}$$

then is

$$\alpha^{(0)}=\alpha=\chi(\rho),\ \alpha^{(1)}=\chi_1(\rho),\ \cdots,\ \alpha^{(n-1)}=\chi_{n-1}(\rho), \tag{3}$$

where the χ's are integral in ρ with rational coefficients.

If the substitution $\sigma=(\rho,\ \rho^{(1)})$ is made, it is seen that

$$F(\alpha)=F[\chi(\rho)]$$

becomes $F[\chi(\rho^{(1)})]$, an expression which is zero, due to the fact that if one root of an irreducible function satisfies an equation, all the roots of this function satisfy the same equation.

It follows that if α is a root of $F(x)=0$, then also $\chi(\rho^{(1)})$ is a root of the same equation. Further (Art. 211) the substitution σ changes no two of the quantities (3) into the same quantity.

We thus have the theorem:

THEOREM. *A substitution σ produces among the roots (3) a certain permutation in that each of the indices 0, 1, $\cdots$, $n-1$ is replaced by a definite one among them.*

We are thus led to study the permutations of n ciphers 0, 1, $\cdots$, $n-1$ and their general properties.

If 0 goes into a_0, 1 into a_1, $\cdots$, $n-1$ into a_{n-1}, then $a_0, a_1, \cdots, a_{n-1}$ is in general another arrangement of the ciphers 0, 1, $\cdots$, $n-1$. The transition from one arrangement to another is called a *permutation* and may

[1] The reader is referred also to Jordan, *Traité des substitutions;* Netto, *Substitutionentheorie;* Weber, *Algebra*, Vol. I, § 155.

be denoted by a symbol

$$\pi_a = \begin{pmatrix} 0, & 1, & 2, & \cdots, & n-1 \\ a_0, & a_1, & a_2, & \cdots, & a_{n-1} \end{pmatrix}.$$

The number of all possible permutations among n elements is $n! = \Pi(n)$, say, this number including the identical permutation

$$\begin{pmatrix} 0, & 1, & 2, & \cdots, & n-1 \\ 0, & 1, & 2, & \cdots, & n-1 \end{pmatrix},$$

in which no element is changed by the permutation.

If by π_b is denoted the permutation

$$\pi_b = \begin{pmatrix} a_0, & a_1, & \cdots, & a_{n-1} \\ b_0, & b_1, & \cdots, & b_{n-1} \end{pmatrix},$$

where $b_0, b_1, \cdots, b_{n-1}$ denotes another arrangement of the numbers $0, 1, \cdots, n-1$, then clearly

$$\pi_a\pi_b = \begin{pmatrix} 0, & 1, & 2, & \cdots, & n-1 \\ b_0, & b_1, & b_2, & \cdots, & b_{n-1} \end{pmatrix}.$$

Observe that in this composition of permutations an interchange in general is not permissible and that is,

$$\pi_a\pi_b \neq \pi_b\pi_a.$$

The associative principle however is applicable, and that is,

$$(\pi_a\pi_b)\pi_c = \pi_a(\pi_b\pi_c).$$

This is clear, if one observes that π_a, say, changes an element p to q while π_b changes q to r and π_c changes r to s. For $(\pi_b\pi_c)$ changes q to s and $\pi_a(\pi_b\pi_c)$ changes p to s, while $(\pi_a\pi_b)$ changes p to r and π_c changes r to s, so that $(\pi_a\pi_b)\pi_c$ changes p to s.

Corresponding to every permutation there is evidently a definite *inverse permutation*, which consists in the fact that through it the change that was produced through the direct permutation is returned to its initial condition; and that is, the inverse permutation of π_a, when com-

pounded with π_a gives the identical permutation. Such an inverse permutation is denoted by π_a^{-1}, so that

$$\pi_a^{-1} = \begin{pmatrix} a_0, & a_1, & \cdots, & a_{n-1} \\ 0, & 1, & \cdots, & n-1 \end{pmatrix}.$$

It is evident that

$$\pi_a \pi_a^{-1} = \begin{pmatrix} 0, & 1, & \cdots, & n-1 \\ 0, & 1, & \cdots, & n-1 \end{pmatrix},$$

and also that

$$\pi_a^{-1} \pi_a = \begin{pmatrix} a_0, & a_1, & \cdots, & a_{n-1} \\ a_0, & a_1, & \cdots, & a_{n-1} \end{pmatrix}.$$

Observe that if

$$\pi_a \pi_b = \pi_c,$$

then

$$\pi_c^{-1} = \pi_b^{-1} \pi_a^{-1};$$

for

$$\pi_a \pi_b (\pi_b^{-1} \pi_a^{-1}) = \pi_a \pi_0 \pi_a^{-1},$$

where π_0 denotes the identical permutation; and further

$$\pi_a \pi_0 \pi_a^{-1} = \pi_a \pi_a^{-1} = \pi_0,$$

while

$$\pi_c \pi_c^{-1} = \pi_0.$$

It is seen that

$$\pi_0 = \pi_0^{-1},$$

so that π_0 is its own inverse.

THEOREM. *If π_c is compounded of π_a and π_b, so that $\pi_a \pi_b = \pi_c$, then not only π_c is known, when π_a and π_b are given, but also π_a is known when π_b and π_c are given, and π_b is fully and uniquely determined from π_a and π_c.*

For

$$\pi_a = \pi_c \pi_b^{-1} \qquad \text{and} \qquad \pi_b = \pi_a^{-1} \pi_c.$$

THEOREM. *A system that is constituted out of some or all of the $\Pi(n) = n!$ permutations of n elements*

$$Q = \pi, \ \pi_1, \ \pi_2, \ \cdots,$$

which is closed and complete in itself, in such a way that any two, and consequently also any arbitrary number of permutations of Q, through composition, offers another

permutation of the system, is called a permutation group. *By the degree of a permutation group is to be understood the number of permutations which constitute it.*

The complex, or set of all the $\Pi(n)$ permutations form such a group. Similarly, the identical substitution forms for itself a group. The groups that are situated between these two limits are studied in the following articles.

As a simple example may be mentioned here the group of *cyclic* or *circular permutations*, or for brevity, the *cyclic group*, which is had, if by any arrangement of the ciphers 1, 2, 3, $\cdots$, n, each cipher is replaced by the following cipher and the last cipher by the first, the permutation being repeated until the original order is restored. Take for example three ciphers and the permutations

$$\pi_1=\begin{pmatrix}1, & 2, & 3\\ 2, & 3, & 1\end{pmatrix}, \quad \pi_2=\begin{pmatrix}1, & 2, & 3\\ 3, & 1, & 2\end{pmatrix}, \quad \pi_0=\begin{pmatrix}1, & 2, & 3\\ 1, & 2, & 3\end{pmatrix}.$$

Note that the number of ciphers is the degree of the cyclic group.

There also exist groups which consist of permutations of such a nature that besides possessing the properties just mentioned, they also have the commutative property; and that is, for all permutations there exist the property $\pi_i\pi_j=\pi_j\pi_i$. In such cases there is a closer analogy with multiplication. Such groups to which the cyclic groups belong are called the *commutative* or *Abelian* groups.

If all the elements of a permutation group Q_1 are contained in a group Q, then Q_1 is called a *divisor* of Q, and Q is said to be *divisible* by Q_1.

ART. **214. The Galois Groups.** Let the roots α, $\alpha^{(1)}$, $\alpha^{(2)}$, $\cdots$, $\alpha^{(n-1)}$ of the equation

$$F(x)=0$$

be expressed as quantities of the normal realm $\Re(\rho)$ of the mth degree in the form (Art. 213)

$$(1) \qquad \alpha = \chi(\rho), \qquad \alpha^{(k)} = \chi_k(\rho). \quad (k=1, 2, \cdots, n-1).$$

If one of the m substitutions, say σ, of the normal realm be applied, then as seen in Art. 211, there exists a certain permutation among the roots $\alpha(=\alpha^{(0)})$, $\alpha^{(1)}$, $\cdots$, $\alpha^{(n-1)}$. To every substitution σ there corresponds a certain permutation π of the ciphers $0, 1, \cdots, n-1$. Different substitutions σ_h, σ_k lead to different permutations π_h, π_k. For, if ρ is a rational function of the α's (see Art. 210), say

$$\rho = \Phi(\alpha, \alpha^{(1)}, \cdots, \alpha^{(n-1)}) = \Phi(\chi(\rho), \chi_1(\rho), \cdots, \chi_{n-1}(\rho)),$$

then also, since ρ satisfies an irreducible equation, it is seen that

$$(2) \qquad \rho^{(k)} = \Phi[\chi(\rho^{(k)}), \chi_1(\rho^{(k)}), \cdots, \chi_{n-1}(\rho^{(k)})].$$

Observe next that if the substitutions σ_h, σ_k produce the same permutations among the α's, so that

$$\chi(\rho^{(h)}) = \chi(\rho^{(k)}), \qquad \chi_s(\rho^{(h)}) = \chi_s(\rho^{(k)}) \qquad (s=1, \cdots, n-1),$$

then from (2) it is clear that also

$$\sigma_h = \sigma_k.$$

If, due to the substitution σ_h there arises a permutation π_h among the roots $\alpha^{(0)}$, $\alpha^{(1)}$, $\cdots$, $\alpha^{(n-1)}$, the permutation π_h is said to *correspond* to the substitution σ_h. To every substitution there corresponds a definite permutation and the number of these permutations, including the identical permutation, which corresponds to the identical substitution, is equal to m.

If to the substitutions σ_h and σ_k there correspond the permutations π_h and π_k, then to the compound substitution $\sigma_h\sigma_k$ there corresponds the compound permutation $\pi_h\pi_k$. For the permutations are the results of the corresponding substitutions upon certain quantities of the realm $\Re(\rho)$, and it is immaterial whether two substitu-

tions one after the other are made or whether the compounded substitution is made at once.

Thus arises the theorem:

THEOREM. *There correspond to the m substitutions of the realm* $\Re(\rho)$, *namely,* $\sigma, \sigma_1, \sigma_2, \cdots, \sigma_{m-1}$, *the m permutations of n ciphers* $\pi, \pi_1, \cdots, \pi_{m-1}$, *and in such a way that to the substitution that is compounded of two substitutions, there corresponds the permutation that is the compound of the corresponding permutations.*

It follows that the permutations $\pi, \pi_1, \cdots, \pi_{m-1}$ form a group. This group may be denoted by P and is called the *Galois group* of the equation $F(x)=0$. If $F(x)$ is irreducible, the group P is called the *Galois group* of each of the realms $\Re(\alpha), \Re(\alpha^{(1)}), \cdots, \Re(\alpha^{(n-1)})$. Note that α is a function of ρ so that any rational function of α is a rational function of ρ, and is therefore subjected to the substitutions σ.

Due to the theorem above, which indicates the relation between the elements of this group and the elements of the substitution group, these two groups are said to be *isomorphic.*

Two groups G and P are said to be *isomorphic* if there exists between them the following correspondence:

1. To every permutation of G there corresponds a permutation of P; and to every permutation of P there corresponds at least one permutation of G.

2. To the product of any two permutations of G there corresponds the product of the corresponding permutations of P.

If to every permutation of P there corresponds only *one* permutation of G, the isomorphism is said to be *holoedric,* while it is *meroedric* if this is not the case.

If a function of the n roots $\alpha, \alpha^{(1)}, \cdots, \alpha^{(n-1)}$ remains unchanged when the roots are subjected to a permutation,

it is said to *allow* or *permit* the permutation. (Art. 211, end.)

The characteristic properties of the Galois group are expressed through the following theorems:

THEOREM I. *If a rational function in* $x_1, x_2, \cdots, x_n$ *becomes zero when for these variables are written* $\alpha, \alpha^{(1)}, \cdots, \alpha^{(n-1)}$, *it also becomes zero when these quantities are subjected to any permutation of the Galois group.*

For, express these roots as functions of ρ (Art. 211), the given rational function in these quantities becoming thereby $\varphi(\rho)$. If $\varphi(\rho)=0$, then also is this equation satisfied by all conjugate values, say $\rho^{(h)}$, of ρ. These conjugate values are brought about by the substitutions σ_h which cause the permutations in question.

THEOREM II. *Every rational function of the n roots* $\alpha, \alpha^{(1)}, \cdots, \alpha^{(n-1)}$ *which permits all the permutations of the Galois group, is a quantity of* $\Re$.

The inverse of this theorem may also be proved. (Jordan, §§ 390–1.) Proofs are also given by Dickson, *Modern Alg. Theories*, pp. 165–166.

For, if the function $\varphi(\rho)$ above remains unchanged by all the substitutions σ of the Galois substitution group, then is φ a quantity of the realm $\Re$. (Art. 211, end.)

Consider next the complex of all rational equations such as

$$\psi(\alpha^{(0)}, \alpha^{(1)}, \cdots, \alpha^{(n-1)})=0,$$

where the α's are roots of $F(x)=0$ and the coefficients belong to $\Re$.

THEOREM III. *If any permutation* π *is applicable to all such equations, then* π *is a permutation of the Galois group; and the Galois group may be defined consequently as the totality of all permutations which are applicable to all rational equations among the roots* $\alpha^{(0)}, \alpha^{(1)}, \cdots, \alpha^{(n-1)}$ *of* $F(x)=0$.

For, due to Art. 50, of Vol. I, ρ may be expressed as a rational (in fact linear) function of $\alpha^{(0)}, \cdots, \alpha^{(n-1)}$ in such a way that the $\Pi(n)$ values which are had through the permutations of the α's are all different.[1]

If $g(t)=0$ is the Galois resolvent of $F(x)=0$, whose root is this ρ, then is

$$g(\rho)=0,$$

where ρ has the form

$$\rho=a_0\alpha^{(0)}+a_1\alpha^{(1)}+\cdots+a_{n-1}\alpha^{(n-1)}.$$

By hypothesis the permutation π is applicable. But every permutation π of the α's in the linear expression just written gives another value of ρ, say $\rho^{(h)}$ which is also a root of $g(t)=0$, and consequently, the permutation π corresponds to a substitution, which changes ρ to $\rho^{(h)}$ of the realm $\Re(\rho)$ and that is, π belongs to the Galois group.

From this is derived the following important theorem:

THEOREM IV. *If P is a group of permutations of the n roots $\alpha^{(0)}, \alpha^{(1)}, \cdots, \alpha^{(n-1)}$, to which the properties of Theorems I and II belong, then is P the Galois group of the equation $F(x)=0$.*

For, due to Theorem III every permutation of P belongs to the Galois group, and hence P is a divisor of this group.

Suppose that there are, say r, permutations of P, and denote them by

$$\pi_1, \pi_2, \cdots, \pi_r. \tag{3}$$

When these permutations are made upon the function

$$\rho=a_0\alpha^{0}+a_1\alpha^{(1)}+\cdots+a_{n-1}\alpha^{(n-1)},$$

the corresponding values may be denoted by

$$\rho_1, \rho_2, \cdots, \rho_r. \tag{4}$$

Apply one of the permutations (3), say π_k, to one of these ρ's, say ρ_i, the result being the same as if $\pi_i\pi_k$ were

[1] See also Serret, § 491; or Netto, § 29.

applied to ρ, and denote the result of this permutation by ρ_i'.

Further, since by hypothesis P is a group, it follows that the compound permutation $\pi_i\pi_k$ is a permutation of P and consequently also ρ_i' must be one of the quantities $\rho_1, \rho_2, \cdots, \rho_r$. Next let π_k operate upon ρ_h and let the result of this permutation be ρ_h'. Then from a theorem of Art. 211, ρ_i' is different from ρ_h' if ρ_i is different from ρ_h.

It follows that the quantities

$$\rho_1', \rho_2', \cdots, \rho_r'$$

are, neglecting the sequence, the same as

$$\rho_1, \rho_2, \cdots, \rho_r.$$

It is evident that the product

$$\bar{g}(t) = (t-\rho_1)(t-\rho_2)\cdots(t-\rho_r)$$

remains unaltered through the permutations of the group P. It follows, since Theorem III is here applicable, that $\bar{g}(t)$ is a rational function of t in $\mathfrak{R}$. As $\bar{g}(t)$ is a divisor of the irreducible function $g(t)$, it is seen that r cannot be less than the degree of the Galois group and P is therefore identical with the Galois group.

If as above the quantities ρ are so chosen as functions of $\alpha, \alpha^{(1)}, \cdots, \alpha^{(n-1)}$ that the quantities $\rho, \rho^{(1)}, \cdots$, which arise through permuting the α's, are all different, then is

$$G(t) = (t-\rho)(t-\rho^{(1)})\cdots,$$

a function in $\mathfrak{R}$.

Each of the quantities $\rho, \rho^{(1)}, \cdots$ is a primitive quantity of the normal realm

$$\mathfrak{N} = \mathfrak{R}(\alpha, \alpha^{(1)}, \cdots, \alpha^{(n-1)}) = \mathfrak{R}(\rho).$$

And therefore each of them is the root of a Galois resolvent of the mth degree. Every m of these quantities are the roots of such an equation. It follows that $G(t)$ which has no equal roots is factorable into irreducible

factors, each of the mth degree. From this it also follows that m is a divisor of $\Pi(n)$, and at the same time m is the degree of the Galois group of $F(x)$.

If the Galois resolvent of an equation $F(x)$ of the nth degree has as its degree the greatest possible value $m=\Pi(n)$, then with Kronecker we say that the equation has no *affect*.[1] The lower the degree m of the Galois resolvent the higher is the affect. The integer $\frac{\Pi(n)}{m}$, whose greatest value is $\Pi(n)$ and least value 1, is called the *degree* of the affect. Thus with equations without affect, this value is 1; and if the affect is $\Pi(n)$, the roots of the equation are contained in the realm $\mathfrak{R}$ and therefore the equation is solved.

If through adjunction of an algebraic quantity to $\mathfrak{R}$ the Galois resolvent becomes reducible, then a Galois resolvent of lower degree may be introduced and the degree of the affect of the equation $F(x)=0$ is increased.

Thus the Galois conception of the problem of solving an equation $F(x)=0$ consists in repeatedly adjoining algebraic quantities of the simplest kind to the stock-realm $\mathfrak{R}$, so that the group is gradually diminished or the affect increased until it reaches its highest degree.

THEOREM. *The general equation of the nth degree has no affect in the realm $\mathfrak{R}$, which consists of the rational functions of the coefficients $a_1, a_2, \cdots, a_n$.*

For $a_1, a_2, \cdots, a_n$ may be regarded as the fundamental symmetric functions of the roots $\alpha, \alpha^{(1)}, \cdots, \alpha^{(n-1)}$. If then $g(t)$ is an irreducible factor of $G(t)$, where the coefficients of $g(t)$ are rational in $a_1, a_2, \cdots, a_n$; and if $g(t)$ vanishes for $t=\rho$, we have, if in $g(\rho)=0$ we write for ρ and the a's their values in terms of the α's, an identical

[1] See Kronecker, *Grundzüge*, §§ 10, 11; and Netto, § 153. The word "affect" was used by Kronecker for the first time in the *Berliner Monatsb.*, 1858, p. 288.

equation. In this equation, however, we may permute the α's at pleasure without changing the α's, while ρ takes each one of the values $\rho, \rho', \rho'', \cdots$ of $G(t)$. Hence $g(t)$ vanishes for all the roots of $G(t)$ and consequently must be identical with $G(t)$.

ART. **215. Transitive and Intransitive Groups.**[1] By means of the Galois group there exists a simple criterion as to whether the equation $F(x)=0$ is reducible or irreducible. For, suppose that $F(x)$ of degree n is reducible, and let $F_1(x)$ be one of its irreducible factors of degree k, say, where $k<n$.

Let the roots of $F_1(x)=0$ be

$$\alpha, \alpha^{(1)}, \cdots, \alpha^{(k-1)}, \tag{1}$$

while the remaining roots of $F(x)=0$ may be denoted by

$$\alpha^{(k)}, \alpha^{(k+1)}, \cdots, \alpha^{(n-1)}. \tag{2}$$

If α_1 is any of the roots (1), while α_2 is one of the roots (2), then in the Galois group P there is no permutation through which α_1 becomes α_2. For by hypothesis

$$F_1(\alpha_1)=0,$$

and if there were in P a permutation through which α_1 were replaced by α_2, then, due to Theorem I, Art. 214, $F_1(\alpha_2)=0$, which is contrary to the hypothesis.

Hence, *through the permutations of P, the roots (1) of $F_1(x)=0$ are only permuted among themselves.*

Reciprocally, if the group P has the property that its permutations change only a part of the roots α, as for example (1) above, among one another, then the product

$$(x-\alpha)(x-\alpha^{(1)})\cdots(x-\alpha^{(k-1)})=F_1(x)$$

permits all permutations of P and consequently (see Theorem II, Art. 214) $F_1(x)$ has rational coefficients in $\mathfrak{R}$, and therefore $F(x)$ is reducible.

[1] See Dickson, *Modern Algebraic Theories*, pp. 168 et seq.

A permutation group is said to be *transitive* if it contains at least one permutation which transforms one arbitrary element into another arbitrary element. On the other hand, if the elements can be distributed into two or more divisions in such a way that through no permutation of the group can one element of one division be transformed into an element of another division, the group is said to be *intransitive.*

Accordingly the theorem to be proved may be stated as follows:

THEOREM. *The equation* $F(x)=0$ *is reducible or irreducible according as its associated Galois group is intransitive or transitive.*

If a part of the elements are so connected that due to permutations of P, every element of one division is transformed into every other element of the division, the elements of this division are said to be *transitively connected.* The different transitively connected systems whose elements are only permuted among their respective divisions by all the permutations of P are called the *systems of intransitivity.*

ART. 216. **Primitive and Imprimitive Groups.**[1] Let $F(x)=0$ be an irreducible equation of the nth degree. It follows that its Galois group P is transitive. Let the roots of $F(x)=0$ be

(1) $$\alpha, \alpha_1, \cdots, \alpha_{n-1}.$$

If the realm $\Re(\alpha)$ is imprimitive and if $\tau=\chi(\alpha)$ is an imprimitive element in it, then is (Art. 209)

$$(t-\tau)(t-\tau^{(1)})\cdots(t-\tau^{(n-1)})=\Phi(t)=\varphi(t)^r,$$

where $\varphi(t)$ is an irreducible function of the sth degree; and consequently

$$n=r\cdot s.$$

[1] See Serret, §§ 530 et seq.; and Netto, Chapt. IV; Weber, *Algebra*, Vol. I, pp. 523 ff.

The roots (1) may accordingly be arranged into s rows of r elements, say,

$$(2)\qquad \begin{cases} A=\alpha,\ \alpha_1,\ \cdots,\ \alpha_{r-1}, \\ B=\beta,\ \beta_1,\ \cdots,\ \beta_{r-1}, \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ S=\sigma,\ \sigma_1,\ \cdots,\ \sigma_{r-1}, \end{cases}$$

such that (see Vol. I, Art. 68)

$$(3)\qquad \begin{aligned} \tau=\chi(\alpha)=\chi(\alpha_1)=\cdots=\chi(\alpha_{r-1}), \\ \tau^{(1)}=\chi(\beta)=\chi(\beta_1)=\cdots=\chi(\beta_{r-1}), \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \tau^{(s-1)}=\chi(\sigma)=\chi(\sigma_1)=\cdots=\chi(\sigma_{r-1}), \end{aligned}$$

where

$$(t-\tau)(t-\tau^{(1)})\cdots(t-\tau^{(s-1)})=\varphi(t),$$

$\varphi(t)$ being the irreducible function above of the sth degree with rational coefficients.

From (3) it is evident that the group P is of such a nature that its permutations change the elements of each row in (2) among themselves and the rows $A, B, \cdots, S$ among themselves, so that in no case can two elements of the same row be changed into two elements of different rows. For, if due to a permutation π of P, two elements α and $\alpha^{(1)}$, say, of the first row were changed into β and σ, two elements of different rows, then, due to this permutation, the equality

$$\chi(\alpha)=\chi(\alpha^{(1)}) \qquad \text{would become} \qquad \chi(\beta)=\chi(\sigma),$$

an equality which is *not* true.

Permutation groups P, which have the property that the permuted elements are distributed into rows of equal number of elements and such that the permutations of P change the elements of the same row among themselves, or rows into rows, are called *imprimitive*. The individual rows $A, B, \cdots, S$ are called the *systems of imprimitivity*.

Permutation groups which do not bring about such a distribution of the elements, are called *primitive groups.*

It is possible that a group is imprimitive in several ways, and that is, that it has entirely different systems of imprimitivity. Take for example the group of the cyclic (circular) permutations of six elements (1, 2, 3, 4, 5, 6).

$$\begin{pmatrix}1,2,3,4,5,6\\2,3,4,5,6,1\end{pmatrix}=\pi_1=\begin{pmatrix}2,3,4,5,6,1\\3,4,5,6,1,2\end{pmatrix}=\text{etc.};$$

$$\begin{pmatrix}1,2,3,4,5,6\\3,4,5,6,1,2\end{pmatrix}=\pi_2=\pi_1\cdot\pi_1=\pi_1^2;$$

$$\begin{pmatrix}1,2,3,4,5,6\\4,5,6,1,2,3\end{pmatrix}=\pi_3=\pi_1^3;$$

$$\begin{pmatrix}1,2,3,4,5,6\\5,6,1,2,3,4\end{pmatrix}=\pi_4=\pi_1^4;$$

$$\begin{pmatrix}1,2,3,4,5,6\\6,1,2,3,4,5\end{pmatrix}=\pi_5=\pi_1^5;$$

$$\begin{pmatrix}1,2,3,4,5,6\\1,2,3,4,5,6\end{pmatrix}=\pi_0=\pi_1^6.$$

Observe, if $A=(1,\ 3,\ 5)$ and $B=(2,\ 4,\ 6)$, that the permutations $\pi_2,\ \pi_2^2,\ \pi_2^3$ interchange the elements of A among themselves and the elements of B among themselves, while $\pi_1,\ \pi_3,\ \pi_5$ interchange A and B; while if $A=(1,\ 4)$, $B=(2,\ 5)$, $C=(3,\ 6)$, the permutations $\pi_3,\ \pi_3^2$ change the elements of A to elements of A, elements of B to elements of B, elements of C to elements of C; and π_1 changes A to B and B to C and C to A; π_2 changes A to C, B to A and C to B.

The imprimitive group being defined as above, we have the theorem:

THEOREM. *An imprimitive realm has an imprimitive group.*

Due to the imprimitivity of the group, there exists an important result for the imprimitive realms:

Let $\psi(x, x_1, \cdots, x_{r-1})$ denote any symmetric function of the r variables, and put

$$(4)\qquad \begin{cases} \omega=\psi(\alpha, \alpha_1, \cdots, \alpha_{r-1}), \\ \omega^{(1)}=\psi(\beta, \beta_1, \cdots, \beta_{r-1}), \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \omega^{(s-1)}=\psi(\sigma, \sigma_1, \cdots, \sigma_{r-1}). \end{cases}$$

If τ is defined as above, it may be proved that ω is a rational function of τ, and consequently belongs to the realm $\Re(\tau)$. For, write

$$\varphi(t)\left(\frac{\omega}{t-\tau}+\frac{\omega^{(1)}}{t-\tau^{(1)}}+\cdots+\frac{\omega^{(s-1)}}{t-\tau^{(s-1)}}\right)=\Phi(t),$$

and observe that any permutation which interchanges the α's with α's the β's with β's, etc., leaves the ω's and τ's unchanged, while any permutation which interchanges ω's with ω's makes the same changes among the τ's, so that in all cases $\Phi(t)$ remains unchanged. It follows from Theorem II of Art. 214 that the coefficients of $\Phi(t)$ are rational numbers.

Writing in the expression above $t=\tau$, it is seen that

$$\omega=\frac{\Phi(\tau)}{\varphi'(\tau)};$$

and that is, *any rational symmetric function of* $\alpha, \alpha_1, \cdots, \alpha_{r-1}$ *is a rational function of* τ. If we apply this to the coefficients of the product

$$(u-\alpha)(u-\alpha_1)\cdots(u-\alpha_{r-1})=\varphi(u, \tau),$$

it is seen that $\varphi(u, \tau)$ is a function integral in u, whose coefficients are rational in τ, where τ is the root of an irreducible equation in $\Re$ of the sth degree. It is thus shown that α, the root originally of the nth degree in $\Re$ becomes the root of an equation of the sth degree in $\Re(\tau)$, where $n=r\cdot s$. An equation $F(x)=0$, whose roots have this

property, is called an *imprimitive equation*. The above result may be expressed as follows:

The imprimitive realm $\Re(\alpha)$ *of the nth degree becomes, through the adjunction of the algebraic quantity* τ, *which satisfies an irreducible equation of the sth degree, a realm* $\Re(\alpha, \tau)$ *of the rth degree where* $r \cdot s = n$.

We may next see whether the imprimitivity of the group is a sufficient condition for the imprimitivity of the realm, and that is, whether in a realm $\Re(\alpha)$ with an imprimitive group there are always imprimitive elements.

Let $F(x) = 0$ be an irreducible equation of the nth degree with an imprimitive group and let the quantities (1) above be the roots of this equation, which are arranged in the series (2), and in such a way that the elements of this series are not separated from one another through the permutations of the group.

Take any symmetric function $\psi(x, x_1, \cdots, x_{r-1})$, such that the values

$$(5) \qquad \begin{cases} y = \Psi(\alpha, \alpha_1, \cdots, \alpha_{r-1}), \\ y_1 = \Psi(\beta, \beta_1, \cdots, \beta_{r-1}), \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ y_{s-1} = \Psi(\sigma, \sigma_1, \cdots, \sigma_{r-1}), \end{cases}$$

are all different from one another.

The possibility of having such values is seen, if we put

$$(6) \qquad \begin{aligned} &\psi(t, A) = (t-\alpha)(t-\alpha_1)\cdots(t-\alpha_{r-1}), \\ &\psi(t, B) = (t-\beta)(t-\beta_1)\cdots(t-\beta_{r-1}), \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &\psi(t, S) = (t-\sigma)(t-\sigma_1)\cdots(t-\sigma_{r-1}), \end{aligned}$$

the right hand side of these expressions being integral in t and rational in τ. From Arts. 49, 50 of Vol. I, it is seen that such values may be given to t that $\psi(t, A), \cdots, \psi(t, S)$ are all different from one another. These values may be taken for the y's in (5).

Let u be an independent variable and put

$$\varphi(u)=(u-y)(u-y_1)\cdots(u-y_{s-1}).$$

Observe that the coefficients of this function remain unchanged when subjected to the permutations of the imprimitive group in question. On account of the presupposed transitivity of the group by which the y's are interchanged, it follows also that $\varphi(u)$ is irreducible.

It is clear from the expression

$$\varphi(u)\left[\frac{\omega}{u-y}+\frac{\omega_1}{u-y_1}+\cdots+\frac{\omega_{s-1}}{u-y_{s-1}}\right]=\Omega(u),$$

if ω is any symmetric function of $\alpha, \alpha_1, \cdots, \alpha_{r-1}$, then by writing $u=y$, that ω is a rational function of y.

It follows that the function $\psi(t, A)$ above is integral in t and rational in y, so that we may write formula (6)

$$\psi(t, A)=(t-\alpha)(t-\alpha_1)\cdots(t-\alpha_{r-1})=\psi(t, y).$$

Further, the function $\psi(t, y)$ is irreducible in $\Re(y)$; for if $\psi_1(t, y)$ is an irreducible factor of $\psi(t, y)$, which vanishes for one of the roots of $\psi(t, y)$, say α, so that $\psi_1(\alpha, y)=0$, then, due to the transitivity of the group, a permutation may be applied by which α is changed into α_1, say, without any change in y. It follows that $\psi_1(\alpha_1, y)=0$ and similarly, every root of $\psi(t, y)$ is also a root of $\psi_1(t, y)$ with the result that $\psi(t, y)$ and $\psi_1(t, y)$ are identical.

It follows further that the equation $F(x)=0$ of the nth degree, is imprimitive in the sense defined above, and that is, a root α of this equation may be regarded as a root of an equation of the rth degree whose coefficients depend upon the root y of an equation of the sth degree.

To show finally that also the realm $\Re(\alpha)$ (in the sense of Art. 209) is imprimitive, it remains to prove that in the realm $\Re(\alpha)$ there exist quantities that satisfy an irreducible equation of the sth degree. As y itself satisfies an irreducible equation of the sth degree, it is only necessary

to show that y belongs to $\Re(\alpha)$ and that is, y is a rational function of α.

To prove this, observe that $\psi(\alpha, y)=0$, while $\psi(\alpha, y_1)$, $\cdots$, $\psi(\alpha, y_{s-1})$ are different from zero. For, were say $\psi(\alpha, y_1)=0$, then α would be a root of an equation of the rth degree $\psi(t, y_1)=0$, whose roots are the r quantities β, $\beta_1, \cdots, \beta_{r-1}$ that are different from α.

It thus becomes evident that the two equations

$$\psi(\alpha, u)=0 \qquad \text{and} \qquad \varphi(u)=0$$

have one and only one root in common, namely, $u=y$. It is seen that the greatest common divisor of these two functions is linear in u and rational in α; and that is, y may be expressed rationally through α.

With this is also proved the theorem:

THEOREM. *A primitive realm has a primitive group.* (See Jordan, §§ 54 ff.)

ART. 217. **Application** [1] **of Permutation Groups to Equations.** A more exact study of the permutation groups is necessary for a deeper penetration into algebraic problems. A new light was thrown on the method of solution of algebraic equations by Cauchy (*Exercises d'analyse et de physique mathématique*) through a consideration of groups of permutations which leave a given rational function of the roots unchanged.

We may first present some general theorems which will form the foundation for the following discussions.

Let

(1) $$u_1, u_2, \cdots, u_n$$

be a system of independent indeterminates (variables), and let

(2) $$\psi(u_1, u_2, \cdots, u_n)$$

be an integral rational function of these quantities with

[1] See Weber's *Algebra*, Vol. I, § 159.

coefficients that belong to an arbitrary realm. Two such functions when arranged in powers and products of the u's are regarded as equal, when the corresponding terms have the same coefficients.

If the indices of the variables, or what is the same thing, if the u's themselves are subjected to a permutation π, the function ψ may either change in value or it may remain unchanged. If it remains unchanged, it is said to *permit* the permutation π. If it permits all $\Pi(n)$ possible permutations, it is a symmetric function and accordingly may be expressed through the fundamental symmetric functions. The other extreme case is when the function takes different values for all the $\Pi(n)$ permutations.

In general, certain permutations leave the function ψ unchanged while others give it different values.

THEOREM I. *The complex or system of all the permutations of* $u_1, u_2, \cdots, u_n$ *which leave an integral function* $\psi(u_1, \cdots, u_n)$ *unchanged, is a group of permutations.*

To prove this, suppose that π is a permutation that leaves ψ unchanged, a fact which may be expressed through

$$\psi = \psi_\pi.$$

Since the u's are independent variables, this identical equation must remain such when the variables are subjected to any permutation π'. But if π' is applied to ψ_π, the result is the same as if the compound permutation $\pi\pi'$ were applied to ψ.

It follows that

$$\psi_{\pi'} = \psi_{\pi\pi'}.$$

Further, if $\psi = \psi_{\pi'}$, it is seen that

$$\psi = \psi_{\pi\pi'};$$

and that is, if the function ψ remains unchanged through the permutation π and π', it remains unchanged also

through $\pi\pi'$, with which, due to the definition of a group, the Theorem I is proved.

By means of this theorem we have a method of forming permutation groups. For take any function ψ of n variables and find all permutations which leave it unchanged. It will be shown later that from this group all permutation groups may be formed.

THEOREM II. *If* $P=\pi, \pi', \pi'', \cdots$ *is a group of permutations on n elements, and if* π_1 *is an arbitrary one of them, then the system*

$$P_1=\pi\pi_1, \pi'\pi_1, \pi''\pi_1, \cdots$$

is, neglecting the sequence, the same as the system P.

For, due to the property of a group of permutations, it is seen that each element of P_1 is an element of P. Further, the elements of P_1 are all different (Art. 213); and as there are the same number of elements in P_1 as in P, it is clear that the system P_1 is, neglecting the sequence, the same as P.

Similarly, it may be proved that

$$P_1'=\pi_1\pi, \pi_1\pi', \pi_1\pi'', \cdots$$

is identical with P.

With this may be proved the following theorem:

THEOREM III. *Every permutation group contains the identical permutation.*

For, among the permutations of P_1 there must also appear the permutation π_1 and if $\pi_0\pi_1=\pi_1$, then π_0 is the identical permutation.

THEOREM IV. *Corresponding to every permutation of a permutation group P there is its inverse, which is an element of the group.*

For, if $\pi\pi_1$ is the identical permutation in P_1, then is

$$\pi\pi_1=\pi_0 \qquad \text{or} \qquad \pi=\pi_0\pi_1^{-1}=\pi_1^{-1},$$

where π_1 is any arbitrary permutation of P.

If instead of the indeterminates $u_1, u_2, \cdots, u_n$ are written definite numerals or quantities of a realm, say $\alpha_1, \alpha_2, \cdots, \alpha_n$, then Theorem I above ceases in its generality to be true. For, take the simple case where $n=3$, and let a relation among $\alpha_1, \alpha_2, \alpha_3$ be $2\alpha_3=\alpha_1+\alpha_2$. The function $\alpha_2-\alpha_3$ remains unchanged through the permutation

$$\begin{pmatrix}1, 2, 3\\ 2, 3, 1\end{pmatrix}=\pi,$$

say, the function becoming

$$\alpha_3-\alpha_1=\alpha_3-2\alpha_3+\alpha_2=\alpha_2-\alpha_3.$$

Further, the identical permutation leaves $\alpha_2-\alpha_3$ unchanged. However, π and π_0 do not form a group, for such a group must contain the element

$$\pi_2=\pi^2=\begin{pmatrix}1, 2, 3\\ 3, 1, 2\end{pmatrix},$$

which is not here the case.

The following theorem is, however, true for such functions:

THEOREM V. *If P is a permutation group of m ciphers, and if $\alpha_1, \cdots, \alpha_m$ are arbitrary quantities that are different from one another, there exist rational functions of these quantities with rational coefficients, which do not change values when the indices of the α's are subjected to a permutation of the group P, and which change values when a permutation that does not belong to the group P is applied to them.*

To prove this take a function

$$\rho=\Phi(\alpha_1, \alpha_2, \cdots, \alpha_m),$$

which has $\Pi(m)$ different values, when the α's are interchanged in all possible ways. Denote the values, which ρ assumes through application of the permutations

of the group P by

(1) $$\rho,\ \rho_1,\ \cdots,\ \rho_{\mu-1}.$$

Due to Theorem II above, neglecting the sequence, these quantities are only changed among themselves, when a permutation π_1 of the group P is applied to them. For, the application of a permutation π_1 to all the functions (1) has the same result as the application of the permutations of P_1 to ρ; and from Theorem II, the groups P and P_1 are identical, neglecting the sequence of their respective elements.

If t is a variable, the function

(2) $$\psi=(t-\rho)(t-\rho_1)\cdots(t-\rho_{\mu-1})$$

remains unaltered when subjected to any permutation of P.

If then the quantities (1) are subjected to a permutation which does not belong to P, they become, say

$$\rho',\ \rho'_1,\ \cdots,\ \rho'_{\mu-1},$$

where at least one of the ρ''s does not appear among the quantities (1). It follows that

$$\psi_1=(t-\rho')(t-\rho'_1)\cdots(t-\rho'_{\mu-1})$$

is *not* identical with ψ.

It is therefore possible to give to t such a rational value, that all functions which have been formed like ψ_1 are different from ψ.

The above results are evidently true, if independent variables enter in the place of the α's.

A function which permits the permutations of a group P, whilst it changes values with all permutations that do not belong to P, is called a *function belonging to the group* P.

To a group P_0, which includes *all* permutations of m ciphers, belong the symmetric functions. This group is therefore called the *symmetric group*.

A function ρ which belongs to the one single group which consists of the identical permutation may serve for the unique symbolizing of the permutations. For, there is only one permutation π' through which ρ becomes ρ'. For this permutation the symbol (ρ, ρ') may be used, so that

$$(\rho, \rho), (\rho, \rho'), (\rho, \rho''), \cdots (\rho, \rho^{(m-1)})$$

may represent symbolically all permutations of m ciphers.

ART. **218. Transpositions. Cycles.** By the *transposition* $(1, 2)$ is to be understood that 1 and 2 are interchanged, so that $(1, 2) = (2, 1)$, while $(1, 1) = (1, 2)(1, 2)$; and that is, a transposition twice repeated leads to the identity. Hence, every transposition is its own inverse.

If

$$\pi = \begin{pmatrix} 1, & 2, & \cdots, & m \\ a_1, & a_2, & \cdots, & a_m \end{pmatrix},$$

then, since the transposition (m, a_m) interchanges m and a_m, it is seen that the compound $\pi(m, a_m) = \pi_1$, say, leaves m unchanged.

Accordingly, we may write

$$\pi_1 = \pi(m, a_m) = \begin{pmatrix} 1, & 2, & \cdots, & m-1 \\ b_1, & b_2, & \cdots, & b_{m-1} \end{pmatrix},$$

which is a permutation of at most $m-1$ ciphers.

Further, since $\pi = \pi_1(m, a_m)$, the following theorem follows through induction:

THEOREM I. *Every permutation may be distributed into transpositions and in an infinite number of different ways.*

THEOREM II. *If a permutation group of n ciphers contains all transpositions with one fixed letter, for example, $(1, 2), (1, 3), \cdots, (1, n)$, the group is identical with the symmetric group.* (Netto, § 34.)

Observe that, if the ciphers in say (1, 2, 3, 4, 5) be subjected to the transposition (1, 2), it becomes (2, 1, 3, 4, 5); and if a transposition (1, 3) be made, the latter expression becomes (2, 3, 1, 4, 5); and if in this, there is a transposition (1, 2), we have (1, 3, 2, 4, 5). This latter expression is the same as if a transposition (2, 3) had been effected in the original arrangement (1, 2, 3, 4, 5). We may therefore write

$$(1, 2)(1, 3)(1, 2) = (2, 3);$$

and similarly,

$$(1, 3)(1, 4)(1, 3) = (3, 4),$$
$$(1, 3)(1, 5)(1, 3) = (3, 5),$$

etc. It is thus seen from Theorem I that every permutation of the symmetric group may be compounded of the transpositions $(1, 2), (1, 3), \cdots, (1, n)$.

A permutation π is called *cyclic* or *circular* when the ciphers can be arranged in a row in such a way that through the permutation π each cipher becomes the following cipher and the last one is again transformed into the first. For example,

$$\begin{pmatrix} 1, & 2, & \cdots, & n-1, & n \\ 2, & 3, & \cdots, & n, & 1 \end{pmatrix}.$$

Such cyclic permutations may be denoted simply by

$$\pi = (1, 2, 3, \cdots, n),$$

it being immaterial which cipher comes first. For example, $\pi = (3, 4, \cdots, n, 1, 2)$, etc.

The *order* of a permutation π is the smallest exponent ν such that $\pi^\nu = 1$, where 1 denotes the identical permutation. It is evident that the order of a cyclic (circular) permutation is equal to the number of letters (n, say) which it displaces. For, arrange the n letters at equal distances around the circumference of a circle and

observe that the substitution must be repeated n times to regain the original position.

THEOREM III. *Every permutation π may be uniquely distributed into a series of cyclic permutations such that no two of these cycles contain the same cipher.* (Serret, § 408; Netto, § 22.)

For, if

$$\pi = \begin{pmatrix} 1, & 2, & \cdots, & n \\ a_1, & a_2, & \cdots, & a_n \end{pmatrix},$$

and if we begin with any arbitrary cipher, say 1, and write down the row 1, $a_1(=b)$, where b is the same cipher in the top row of π as a_1 is in the bottom, we have, say

$$1,\ a_1(=b),\ a_b,\ a_b(=c),\ a_c,\ \cdots \tag{1}$$

a series which continues until we come to a cipher which has already appeared. This cipher must be 1. For every preceding cipher in the series (1) is uniquely determined through π.

The ciphers $(1, b, c, \cdots)$ form the first cycle. If all the ciphers of π have not appeared in this cycle, take one of the remaining and continue in the same way until all the ciphers of π have been used. Observe that in these cycles, corresponding to any cipher the preceding as well as the succeeding ciphers are uniquely determined through π. It is clear that the cycles themselves are uniquely determined. A cipher, which does not change, forms a one term cycle. The following examples serve as illustrations:

$$\pi_1 = \begin{pmatrix} 1, 2, 3, 4, 5, 6, 7, 8 \\ 3, 6, 7, 1, 4, 5, 8, 2 \end{pmatrix} = (1, 3, 7, 8, 2, 6, 5, 4).$$

$$\pi_2 = \begin{pmatrix} 1, 2, 3, 4, 5, 6, 7, 8 \\ 2, 1, 3, 5, 7, 8, 6, 4 \end{pmatrix} = (8, 4, 5, 7, 6)(1, 2)(3).$$

$$\pi_3 = \begin{pmatrix} 1, 2, 3, 4, 5, 6, 7, 8 \\ 2, 3, 6, 5, 8, 1, 4, 7 \end{pmatrix} = (8, 7, 4, 5)(1, 2, 3, 6).$$

Note that the sequence of cycles is of the same meaning as of a composition and that permutations which have no cipher in common may be interchanged. One term cycles which change nothing are often left out.

In general if π and κ are two permutations of n ciphers, $\kappa\pi$ is different from $\pi\kappa$. It follows that

$$\pi^{-1}\kappa\pi = \kappa' \neq \kappa.$$

If κ is distributed into its cycles, κ' may be derived from κ, giving rise to the following theorem:

THEOREM IV. *The permutation $\pi^{-1}\kappa\pi$ is had, if the permutation π is applied to the cycles of κ.*

To prove this let κ be distributed into its cycles, say,

$$\kappa = (\alpha, \beta, \gamma, \cdots)(\alpha', \beta', \gamma', \cdots)\cdots$$

and let

$$\pi = \begin{pmatrix} \alpha, & \beta, & \gamma, & \cdots, & \alpha', & \beta', & \gamma', & \cdots \\ \alpha_\pi, & \beta_\pi, & \gamma_\pi, & \cdots, & \alpha'_\pi, & \beta'_\pi, & \gamma'_\pi, & \cdots \end{pmatrix}.$$

Through π^{-1}, α_π becomes α, and through κ, α becomes β; and through π it is seen that β becomes β_π. Hence, α_π through $\pi^{-1}\kappa\pi$ becomes β_π. The same permutation changes β_π to γ_π, etc., with the result that

$$\pi^{-1}\kappa\pi = (\alpha_\pi, \beta_\pi, \gamma_\pi, \cdots)(\alpha'_\pi, \beta'_\pi, \gamma'_\pi, \cdots)\cdots$$

and with this is proved Theorem IV. (Weber, *Algebra*, Vol. I, p. 536; see also Dickson, *Mod. Alg. Theories*, p. 186; Fricke, *Die elliptischen Funktionen*, etc., Part II.)

ART. 219. **Permutations of the First and the Second Kinds.** Let $a_1, a_2, \cdots, a_n$ be real quantities such that $a_1 > a_2 > a_3 \cdots > a_n > 0$ and form the product of the differences of these quantities:

$$\begin{aligned} P(a_1, a_2, \cdots, a_n) \equiv P = {} & (a_1 - a_2)(a_1 - a_3)\cdots(a_1 - a_n) \\ & \times (a_2 - a_3)\cdots(a_2 - a_n) \\ & \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ & \times (a_{n-1} - a_n). \end{aligned}$$

If the indices are changed in any manner whatever, then P becomes, say

$$P' = (a_{\alpha_1} - a_{\alpha_2})(a_{\alpha_1} - a_{\alpha_3}) \cdots (a_{\alpha_1} - a_{\alpha_n})$$
$$\times (a_{\alpha_2} - a_{\alpha_3}) \cdots (a_{\alpha_2} - a_{\alpha_n})$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\times (a_{\alpha_{n-1}} - a_{\alpha_n}).$$

THEOREM I. *Through a simple transposition* (h, k), *where* h *and* k *denote any of the ciphers* $1, 2, \cdots, n$, *both* P *and* P' *change signs.*

Take for example the transposition (1, 2) and observe that the two first rows in P become, due to this transposition,

$$(a_2 - a_1)(a_2 - a_3) \cdots (a_2 - a_n)$$
$$(a_1 - a_3) \cdots (a_1 - a_n),$$

the other rows remaining unchanged. Further, observe that these products are the same as those found in the two first rows of P with the only exception of $(a_2 - a_1)$ which has the opposite sign of the corresponding term in P. All the terms containing h and k may be arranged in the same scheme as the arrangement in P of the terms containing 1 and 2. The theorem is thus proved.

By definition *permutations of the first kind* are those that leave the product P unchanged, while the *permutations of the second kind* change P to $-P$. We have at once:

THEOREM II. *The permutations of the first kind are the compounds of an even number of transpositions and those of the second kind of an odd number.*

Belonging to the first kind is to be reckoned the so-called identical permutation which leaves P unchanged.

A further consequence is that in whatever way a product P' is derived from P by means of transpositions, the number of transpositions is always even or odd, according as P' has the same or opposite sign of P.

If in each of the totality of arrangements

$$A, A', A'', \cdots$$

of n elements, a transposition is made, say (1, 2), then each of these arrangements goes into another definite arrangement, say A into B, A' into B', etc., and if the same transposition is repeated, then B returns to A, B' to A', etc. From this it follows that the arrangements B are all different from one another and consequently in their totality are the same as the totality of the A's.

Further, as shown above, all the difference products

$$P, P', P'', \cdots$$

which are formed from P with the different arrangements $A, A', A'', \cdots$ change sign through a transposition. It follows that to each A of the first kind there corresponds a definite B of the second kind, and to each A of the second kind, there is a definite B of the first kind with the result:

THEOREM III. *The number of arrangements of the first kind is the same as the number of arrangements of the second kind, and that is* $=\frac{1}{2}\Pi(n)$.

For $n=3$ we have the following six arrangements

(1, 2, 3)	(2, 3, 1)	(3, 1, 2)
(3, 2, 1)	(2, 1, 3)	(1, 3, 2),

of which the first horizontal row forms the first kind. Observe that (1, 2)(1, 3) changes (1, 2, 3) to (2, 3, 1), etc.

The above theorem was proved through a consideration of the product P. In the sequel it will be shown that the same results may be had without the use of such a function. To bring about this, it may be proved that if τ denotes a transposition, and if π is an arbitrary permutation, then in the compound $\tau\pi$ the number of cycles is either one greater or one less than in the permutation π. For, the two ciphers which are interchanged through τ

may either appear in the same cycle, or they may fall in different cycles. Suppose

1°, that the cycle

$$\gamma=(1, 2, \cdots, a, a+1, \cdots, b)$$

appears in π and suppose that τ operates on two ciphers that appear in γ, say $\tau=(1, a)$. We may write γ in the form

$$\gamma=\begin{pmatrix}1, & 2, & \cdots, & a-1, & a, & a+1, & \cdots, & b\\ 2, & 3, & \cdots, & a, & a+1, & a+2, & \cdots, & 1\end{pmatrix}$$

and

$$\tau\gamma=\begin{pmatrix}a, & 2, & 3, & \cdots, & a-1, & 1, & a+1, & \cdots, & b\\ 2, & 3, & 4, & \cdots, & a, & a+1, & a+2, & \cdots, & 1\end{pmatrix}.$$

From this it is clear that the number of cycles has been increased by one, while the remaining cycles in π have remained unchanged. Suppose, however,

2°, that the two ciphers that are interchanged by τ fall in two different cycles of π, say in

$$\gamma=(1, 2, \cdots, a) \qquad \text{and} \qquad \gamma'=(1', 2', \cdots, a'),$$

and suppose that $\tau=(1, 1')$. It follows that

$$\gamma\cdot\gamma'=\begin{pmatrix}1, & 2, & 3, & \cdots, & a-1, & a, & 1', & 2', & \cdots, & a'-1, & a'\\ 2, & 3, & 4, & \cdots, & a, & 1, & 2', & 3', & \cdots, & a', & 1'\end{pmatrix}$$

and

$$\tau\gamma\gamma'=\begin{pmatrix}1', & 2, & 3, & \cdots, & a-1, & a, & 1, & 2', & \cdots, & a'-1, & a'\\ 2, & 3, & 4, & \cdots, & a, & 1, & 2', & 3', & \cdots, & a', & 1'\end{pmatrix}.$$

It is evident that through the compound $\tau\gamma\gamma'$ the two cycles γ and γ' have merged into one, while the remaining cycles in π have remained unchanged.

Next, let π be a permutation on m ciphers, which consists of ν cycles (including the one-term cycles), which have been brought about through μ transpositions. These cycles may through such transpositions in the inverse order be changed into the identical permutation.

This identical permutation consists of m one-term cycles. Therefore in all $m-\nu$ cycles have been thereby gained; and since each transposition effects the gain or loss of one cycle, it follows that the number of transpositions is $\mu=g+l$, where g is the total number of cycles gained, l being the total number lost. Further, the differences in the number of cycles gained over those lost is $g-l$ which is $m-\nu$ above. It follows that

$$\mu-(m-\nu)=2l \qquad \text{or} \qquad \mu\equiv(m-\nu) \pmod 2.$$

It is thus clear that μ is an odd or even integer according as $m-\nu$ is odd or even. The number $m-\nu$, however, is inherent in the permutation and does not depend upon the method of its distribution into cycles.

EXAMPLE. Prove that the μth power of a cyclic permutation π of order ν is itself cyclic if $(\mu, \nu)=1$; but if $(\mu, \nu)=d>1$, then π^{μ} is a permutation composed of d cycles of order $\frac{\nu}{d}$.

We further have:

THEOREM IV. *The permutations of m ciphers fall into two classes of which the first may be distributed into an even number of transpositions and the second class into an odd number of transpositions.*

Each of these two classes contains an equal number of permutations $=\frac{1}{2}\Pi(m)$. For, through the applications of any transposition all the permutations of the first class become permutations of the second class and *vice versa*. (Serret, § 429; Netto, § 35.)

The composition of two permutations of the first kind is a permutation of the first kind while a permutation of the first kind compounded with one of the second kind offers a permutation of the second kind. We therefore have:

THEOREM V. *The permutations of the first kind form a group.*

A function of m variables $u_1, \cdots, u_m$ or of m quantities $\alpha_1, \cdots, \alpha_m$ that are all different from one another, which changes sign when any two of the variables are interchanged, for example, the product of the differences

$$(u_1-u_2)(u_1-u_3)\cdots(u_1-u_m)$$
$$\times(u_2-u_3)\cdots(u_2-u_m)$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

is called an *alternating function*. Such a function when operated upon by a permutation of the first kind remains unchanged, while it changes sign when any permutation of the second kind is applied to it. The alternating functions, therefore, belong to the group of permutations of the first kind.

Previously (Art. 217) we have called the group to which the symmetric functions belong, the symmetric group; so here we shall call the group to which the alternating functions belong, the *alternating group*. (See Jordan, pp. 61 ff.) The group which consists of one single identical permutation may be called the *identical group* or also the *unit group*.

A cyclic permutation of n ciphers may be distributed into $n-1$ transpositions as follows:

$$(1, 2, \cdots, n) = (1, 2)(1, 3)\cdots(1, n).$$

From this it is evident that a cyclic permutation belongs to the first or the second kind according as n is odd or even. (See Serret, § 422.)

Observe that two transpositions in which the same cipher occurs, are such that $(1, 2)(1, 3) = (1, 2, 3)$, while two transpositions in which the ciphers are all different are exemplified through $(1, 4)(2, 3) = (1, 2, 3)(1, 2, 4)$. It is clear that all permutations of the first kind may be replaced by cycles of three ciphers.

And this gives rise to the following theorem:

THEOREM VI. *All permutations of the first kind may be distributed in an infinite number of ways into cyclic permutations of three elements.*

Next observe that every cycle of three ciphers may be compounded of cycles with three ciphers of which two are fixed. For example

$$(2, 1, 3) = (1, 2, 3)(1, 2, 3),$$
$$(1, 3, 4) = (1, 2, 3)(2, 1, 4)(2, 1, 3),$$
$$(2, 4, 5) = (2, 1, 4)(1, 2, 5)(1, 2, 4),$$
$$(3, 4, 5) = (2, 1, 3)(2, 4, 5)(1, 2, 3).$$

An immediate consequence is the following:

THEOREM VII. *Every permutation group that contains all cyclic permutations of three letters of which two are fixed, must contain the alternating group.*

THEOREM VIII. *If m is greater than 4, then every permutation group of m ciphers, which contains all permutations (1, 2)(3, 4) of two transpositions with no cipher in common, is divisible by the alternating group.* (Netto, Theorem IX, § 35.)

For, observe that

$$(1, 2, 3) = (1, 2)(4, 5)(4, 5)(1, 3);$$

and, if there is a fifth cipher besides 1, 2, 3, 4, it is clear that all cycles of three ciphers may be compounded of pairs of transpositions of the form (1, 2)(4, 5).

If, however, $m = 4$, then the four permutations

$$(1),\ (1, 2)(3, 4),\ (1, 3)(2, 4),\ (1, 4)(2, 3)$$

form a group which is smaller than the alternating group, since the latter contains besides these permutations also the eight cycles

$$(1, 2, 3),\ (1, 2, 4),\ (1, 3, 2),\ (1, 4, 2),$$
$$(1, 3, 4),\ (1, 4, 3),\ (2, 3, 4),\ (2, 4, 3).$$

To the above theorems may be added the following, which have to do with transitive permutation groups:

THEOREM IX. *If a transitive permutation group of m ciphers contains at least one transposition, it is either the symmetric group or it is imprimitive.*

Let the permutation group on m ciphers in question be denoted by P, the ciphers being $1, 2, \cdots, m$, and let the transposition $(1, 2)$ be among the permutations of P. Suppose also that the transpositions $(1, 3), \cdots, (1, \mu)$ and no other transposition with the cipher 1, belong to P. If $\mu = m$, then, due to the Theorem II, Art. 218, P is the symmetric group. If however, $\mu < m$, then, due to the same theorem, P contains all permutations of the ciphers

$$M = 1, 2, \cdots, \mu.$$

From this it follows that P contains no transpositions of one of the ciphers, $1, 2, \cdots, \mu$ with another cipher, say, $\mu+1$. For, if $(2, \mu+1)$ appeared in P, then also $(1, 2)(2, \mu+1)(1, 2) = (1, \mu+1)$ would appear in P, which is contrary to the assumption.

Next, if P is a transitive group, there exists in it a permutation π (that is not a transposition) which transforms the cipher 1 into a cipher that is not one of the ciphers in M, say $\mu+1$; and when operated upon by π, no one of the ciphers of M can become another cipher of M. If, for example, due to π the cipher 2 becomes r, where r is a cipher of M, then $\pi^{-1}(1, 2)\pi$ operating on $(r, \cdots, \mu-1)$ changes these ciphers to $(\mu+1, \cdots, r)$, so that

$$\pi^{-1}(1, 2)\pi = (\mu+1, r),$$

which is a transposition in which r, one of the ciphers of M, is changed into one of the ciphers $\mu+1, \mu+2, \cdots, m$, contrary to what has just been proved.

Thus it is seen that through each permutation of P, the ciphers of M are only changed among themselves, or, they are changed into an entirely different system of ciphers, say M'.

If there are other ciphers that do not appear in either M or M', there exists a permutation in P through which the ciphers of M are transformed into ciphers of a third system M'' in which there is no cipher that occurs in either M or M'. For, let there be two ciphers of M, say α and β (which may also be identical) and suppose that through the permutations π and π' these two ciphers are transposed into a cipher γ, which appeared in both M and M'', then β would, through the permutation $\pi_1 = \pi'\pi^{-1}$ be transposed into α. Hence, the permutation π_1 can only transpose the ciphers of M among themselves; and, since $\pi' = \pi_1\pi$, it follows that M' and M'' must be identical.

Thus it is seen that all the ciphers $1, 2, \cdots, m$ are distributed into systems $M, M', M'', \cdots$, there being μ ciphers in each system which through P are permuted imprimitively; and that is, P is an imprimitive group.

If m is a prime integer, there exist no imprimitive permutation groups, with the result that in this case a transitive group which contains a transposition can be only the symmetric group.

In a similar manner and from Theorem VII, may be derived the following:

THEOREM X. *If a transitive permutation group of $m(>4)$ ciphers contains one or more cycles of three ciphers, it either contains the entire alternating group or it is an imprimitive group.*

For, if the group P contains the cycles of three ciphers

$$(1, 2, 3),\ (1, 2, 4),\ \cdots,\ (1, 2, \mu),$$

but no other cycle of three letters having the ciphers 1, 2, then, due to Theorem VII, it contains the entire alternating group of the ciphers

$$M = 1, 2, \cdots, \mu.$$

If $\mu < m$, there cannot appear in P a cycle of three ciphers which connect one or two of the ciphers M with other ciphers. For, let P contain a permutation $(1, r, s)$, such that of the two ciphers r, s, at least one does not appear in M and choose from M two ciphers α and β so that neither α nor β is the same as one of the ciphers $1, r, s$. Then observe that

$$(1, \beta, \alpha)(1, r, s)(1, \alpha, \beta) = (\alpha, r, s).$$

Note that $(1, \alpha, \beta)$ is the inverse of $(1, \beta, \alpha)$ and belongs to P and accordingly, (α, r, s) belongs to P for every α of M. Hence, from Theorem VII it follows that the entire alternating group of ciphers

$$1, 2, 3, \cdots, \mu, r, s,$$

is contained in P, contrary to the hypothesis.

Hence the m ciphers of P, as in the previous case, are distributed into several systems M, M', M'', $\cdots$ of imprimitivity.

We may finally add the theorem:

THEOREM XI. *If the case of imprimitivity occurs in Theorem IX, the group P contains the entire symmetric group for each system of imprimitivity, and likewise in Theorem X, it contains the entire alternating group for each system of imprimitivity.*

The repeated composition of one and the same permutation with itself is denoted by powers of the permutation. If π is any permutation, then in the series

$$\pi^0, \pi^1, \pi^2, \pi^3, \cdots,$$

where $\pi^0 = 1$ is the identical permutation, the same permutation must be necessarily repeated.

From $\pi^{\mu+e} = \pi^\mu$ it follows that $\pi^e = 1$. If e is the smallest positive exponent for which $\pi^e = 1$, the permutations

$$1, \pi, \pi^2, \cdots, \pi^{e-1}$$

are all different from one another, while

$$\pi^e,\ \pi^{e+1},\ \cdots,\ \pi^{2e-1}$$

are periodically repeated in the same sequence. Either of these series is called the *period* of the permutation π, and e is called the *degree* of π.

The period of π constitutes a group, since through composition of any two of its elements another element of the same period arises.

If π is a cyclic permutation,

$$\pi = (1,\ 2,\ \cdots,\ n);$$

then, if n is an even integer,

$$\pi^2 = (1,\ 3,\ \cdots,\ n-1)(2,\ 4,\ \cdots,\ n);$$

and if n is odd

$$\pi^2 = (1,\ 3,\ \cdots,\ n,\ 2,\ 4,\ \cdots,\ n-1),$$

and the degree of π is in both cases n.

For example, let

$$\pi = \begin{pmatrix} 1, & 2, & 3, & 4, & 5, & 6 \\ 2, & 3, & 4, & 5, & 6, & 1 \end{pmatrix} = \begin{pmatrix} 2, & 3, & 4, & 5, & 6, & 1 \\ 3, & 4, & 5, & 6, & 1, & 2 \end{pmatrix}.$$

It follows that

$$\pi^2 = \begin{pmatrix} 1, & 2, & 3, & 4, & 5, & 6 \\ 3, & 4, & 5, & 6, & 1, & 2 \end{pmatrix} = (1,\ 3,\ 5)(2,\ 4,\ 6).$$

If

$$\pi = \begin{pmatrix} 1, & 2, & 3, & 4, & 5, & 6, & 7 \\ 2, & 3, & 4, & 5, & 6, & 7, & 1 \end{pmatrix} = \begin{pmatrix} 2, & 3, & 4, & 5, & 6, & 7, & 1 \\ 3, & 4, & 5, & 6, & 7, & 1, & 2 \end{pmatrix},$$

it is seen that

$$\pi^2 = \begin{pmatrix} 1, & 2, & 3, & 4, & 5, & 6, & 7 \\ 3, & 4, & 5, & 6, & 7, & 1, & 2 \end{pmatrix} = (1,\ 3,\ 5,\ 7,\ 2,\ 4,\ 6).$$

If π is distributed into several cycles, the *degree* of π is equal to the least common multiple of the numbers of the elements in the individual cycles. For example, if $\pi = (1,\ 2)(3,\ 4,\ 5)$, the degree of π is 6.

Writing π in the form

$$\pi = (1, 2)(3, 4, 5) = \begin{pmatrix} 2, & 1, & 4, & 5, & 3 \\ 1, & 2, & 5, & 3, & 4 \end{pmatrix},$$

or

$$\pi = \begin{pmatrix} 1, & 2, & 5, & 3, & 4 \\ 2, & 1, & 3, & 4, & 5 \end{pmatrix},$$

observe that

$$\pi^2 = \begin{pmatrix} 1, & 2, & 3, & 4, & 5 \\ 1, & 2, & 5, & 3, & 4 \end{pmatrix} = (1)(2)(3, 5, 4);$$

$$\pi^3 = \begin{pmatrix} 1, & 2, & 3, & 4, & 5 \\ 2, & 1, & 3, & 4, & 5 \end{pmatrix} = (1, 2)(3)(4)(5);$$

$$\pi^4 = (1)(2)(3, 4, 5); \qquad \pi^5 = (1, 2)(3, 5, 4); \qquad \pi^6 = 1.$$

ART. 220. **Divisors of Groups; Sub-Groups and Conjugate Groups.** In Art. 217 it was seen that a function of n independent variables $u_1, \cdots, u_n$ determined always a permutation group and it was observed that this was not always true if in the place of the variables there entered definite quantities $\alpha_1, \cdots, \alpha_n$. This difference is brought into evidence by the Galois theory which goes to the essence of the question. (See Weber, *Algebra*, Vol. I, pp. 542 ff.)

As in Art. 214 let $F(x) = 0$ be any equation of the nth degree whose coefficients belong to $\mathfrak{R}$, and let its roots be $\alpha, \alpha^{(1)}, \cdots \alpha^{(n-1)}$, which we suppose are all different.

The normal realm $\mathfrak{R}(\alpha, \alpha^{(1)}, \cdots, \alpha^{(n-1)}) = \mathfrak{R}(\rho)$ may be denoted by $\mathfrak{N}$.

By the Galois group P of the realm $\mathfrak{N}$, or of the equation $F(x) = 0$, we may understand either the group of substitutions of the realm $\mathfrak{N}$ or the permutation group of the indices of the α's, which group is isomorphic with the substitution group (Art. 214).

Let p be the degree of P, and that is of the Galois resolvent, and denote the operations of P (whether they

be the substitutions of $\mathfrak{N}$ or the permutations of the α's) by

$$P = \pi,\ \pi_1,\ \cdots,\ \pi_{p-1}. \tag{1}$$

If the system of permutations

$$Q = k,\ k_1,\ \cdots,\ k_{q-1} \tag{2}$$

that are contained in P, form a group, and that is, if any two of these elements of Q, when compounded, form a permutation of Q, the group Q is said to be a *divisor* or *sub-group* of P.

The following important general property may be derived for the divisors of a group:

When the degree q of the divisor Q is less than p, the degree of P, we may take a permutation π_1 of P, that is not an element of Q, and form the system

$$Q\pi_1 = k\pi_1,\ k_1\pi_1,\ \cdots,\ k_{q-1}\pi_1, \tag{3}$$

which may be expressed symbolically as the product $Q\pi_1$.

The elements of (3) are different from the elements of Q. For, were $k\pi_1 = k_1\pi_1$, then is $k\pi_1\pi_1^{-1} = k_1\pi_1\pi_1^{-1}$ or $k = k_1$. Were $k = k_1\pi_1$, then is $k_1^{-1}k = k_1^{-1}k_1\pi_1 = \pi_1$ and as both k and k_1^{-1} belong to Q, it would follow that π_1 is an element of Q, contrary to the assumption. The elements of $Q\pi_1$ do *not* form a group;[1] otherwise $k_1\pi_1 k_2\pi_1 = k_h\pi_1$, where k_h is an element of Q. It would follow that $\pi_1 = k_1^{-1}k_h k_2^{-1}$, which again requires that π_1 be an element of Q.

The system $Q\pi_1$ is called a *sub-group* of Q (within P). The sub-groups remain unaltered if π_1 in (3) is replaced by any element $k\pi_1$ where k is an element of Q, since Qk is identical with Q.

If in general we call any system $Q\pi$ a sub-group, and if among these sub-groups we include Q, it may be proved that two sub-groups are either identical or they have no element in common. For, were $Q\pi_1$ and $Q\pi_2$ two sub-

[1] The terminology "sub-group" is accordingly somewhat of a misnomer.

groups and if $k_1\pi_1 = k_2\pi_2$, where k_1 and k_2 are two elements of Q, it would follow, if we put $k = k_2^{-1}k_1$, that $\pi_2 = k\pi_1$. Since k belongs to Q, it would also follow that

$$Q\pi_2 = Qk\pi_1 = Q\pi_1.$$

If through (2) and (3) the group P is not exhausted, we may form further sub-groups $Q\pi_2, \cdots$, and continue until P is entirely distributed into sub-groups. As each of these sub-groups contains q elements, we have the following important theorems of Lagrange and Cauchy:

THEOREM I. *The degree q of a divisor Q of a group P is a divisor of the degree p of P.*

A corollary of this theorem is: *The degree of any element* (cycle) *of the group* (see preceding article) *is always a divisor of the degree of the group.*

Reciprocally, *if p is a prime integer, every group whose degree is divisible by p will contain a permutation of the pth degree.* (Jordan, §§ 39 and 40.)

The distribution of P into its sub-groups may be well expressed after Galois through the symbolic equation

$$(4)\quad P = Q + Q\pi_1 + Q\pi_2 + \cdots + Q\pi_{j-1}, \qquad \text{where} \qquad p = q \cdot j.$$

The integer j is called the *index* of the divisor Q. This number does not express any peculiar intrinsic property of the group Q but merely a relation of Q to P. As seen above, two sub-groups to Q either are identical or they have no element in common. We thus have the following:

THEOREM II. *If π is any permutation of P, the system of sub-groups*

$$Q\pi,\ Q\pi_1\pi,\ Q\pi_2\pi,\ \cdots,\ Q\pi_{j-1}\pi$$

is different only in sequence from the system

$$Q,\ Q\pi_1,\ Q\pi_2,\ \cdots,\ Q\pi_{j-1}.$$

The definition of sub-groups may be extended to systems of the form πQ, and P may also be distributed

into such systems. Corresponding to the distribution (4) there follows in particular a second distribution

$$P = Q + \pi_1^{-1}Q + \pi_2^{-1}Q + \cdots + \pi_{f-1}^{-1}Q. \tag{5}$$

For, if π_1 does not appear in Q, then π_1^{-1} is not found in Q; and we may form as a first sub-group $\pi_1^{-1}Q$. If π_2 does not enter in $Q\pi_1$, then π_2^{-1} does not appear in $\pi_1^{-1}Q$. For, were $\pi_2^{-1} = \pi_1^{-1}k$, it would follow that $\pi_2 = k^{-1}\pi_1$ which is, contrary to hypothesis, a permutation in $Q\pi_1$. It appears in the treatment of algebraic problems that preference must be given to the distribution (4) over (5).

A quantity ψ of the realm $\mathfrak{R} = \mathfrak{R}(\rho)$ is said to belong to the group Q (within P), if ψ does *not* change when an operation of Q is applied to it, and if it does change when a permutation of P other than of Q is applied to it. The conception of "belonging to" is somewhat extended when compared to that defined in Art. 217, in that the permutations that lie without P are not considered here. When, however, P is the symmetric group, the two definitions are co-extensive.

THEOREM III. *To every divisor Q of P belongs a quantity in $\mathfrak{R}$, and every quantity in $\mathfrak{R}$ belongs to a definite divisor Q of P.*

The first part of the theorem is proved in Theorem V, Art. 217. For, if a function of the α's within a symmetric group belongs to a group Q, it belongs to Q also within any other group P of which Q is a divisor.

The second part of the theorem follows directly from the fundamental property of the Galois group. To show this, we may introduce the following notation: If the permutation π of the group P operates upon a function ψ of $\mathfrak{R}$, then the notation ψ/π denotes this operation. If upon ψ/π a permutation π' is caused to operate, the result is the same as if the compound permutation $\pi\pi'$

operated upon ψ; and that is,

$$(\psi/\pi)\pi' = \psi/\pi\pi'.$$

If ψ remains unchanged when subjected to the permutation π_1, then is

$$\psi = \psi/\pi_1.$$

Due to Theorem I of Art. 215 every permutation π of P may be applied to any equation $\psi - \psi/\pi_1 = 0$ giving $\psi/\pi = \psi/\pi_1\pi$. If then $\psi/\pi = \psi$, it follows that $\psi/\pi_1\pi = \psi$; and that is, the permutations which leave ψ unaltered form a group.

Next, observe that if ψ is a function in $\mathfrak{N}$ which belongs to the group Q, and that is, if

$$\psi = \psi/k = \psi/k_1 = \cdots = \psi/k_{q-1},$$

and if, further, π_1 is any permutation of P which is not found in Q, then

$$\psi/k\pi_1 = \psi/k_1\pi_1 = \cdots = \psi/k_{q-1}\pi_1 = \psi_1,$$

where ψ_1 is different from ψ.

Reciprocally, if for any permutation

$$\psi_1 = \psi/\pi = \psi/k\pi_1 = \cdots, \tag{A}$$

then π must be one of the permutations in the series

$$k\pi_1,\ k_1\pi_1,\ \cdots,\ k_{q-1}\pi_1.$$

For, applying π^{-1} to the expression in (A), it is clear that $k\pi_1\pi^{-1}$ is a permutation which leaves ψ unchanged; and that is, a permutation of the group Q, say k_i. It follows that $\pi = k_i^{-1}k\pi_1$, which is a permutation of $Q\pi_1$.

We therefore have the following:

THEOREM IV. *A function ψ which belongs to Q is transformed through all the permutations of a sub-group $Q\pi$ and through no other permutation of P into a definite quantity ψ_1, which is different from ψ.*

Accordingly, there correspond to the j sub-groups the j functions

$$\psi, \psi_1, \cdots, \psi_{j-1};$$

and from Theorem II follows the theorem:

THEOREM V. *The quantities $\psi, \psi_1, \cdots, \psi_{j-1}$ undergo a permutation, if one and the same operation π of P is applied simultaneously to them all.*

For, the quantities $\psi, \psi_1, \cdots, \psi_{j-1}$ may be expressed in the form $\psi/k, \psi/k\pi_1, \cdots, \psi/k\pi_{j-1}$; and when π is applied to these quantities, we have $\psi/k\pi, \psi/k\pi_1\pi, \cdots, \psi/k\pi_{j-1}\pi$, where k and π are arbitrary permutations of Q and P, respectively. In each of the series

$$k, k\pi_1, \cdots, k\pi_{j-1}$$

and

$$k\pi, k\pi_1\pi, \cdots, k\pi_{j-1}\pi,$$

there is offered from each of the sub-groups $Q, Q\pi_1, \cdots, Q\pi_{j-1}$, one and only one permutation.

The functions $\psi, \psi_1, \psi_2, \cdots, \psi_{j-1}$ which, as shown above, are all different from one another, are called *conjugate functions*. It is easy to determine the group to which each of these individual functions belongs. For, if $\psi_1 = \psi/\pi_1$, and if π is a permutation of P which leaves ψ_1 unchanged, then is

$$\psi/\pi_1\pi = \psi_1/\pi = \psi_1 = \psi\pi_1.$$

Apply to this expression the permutation π_1^{-1} which belongs to P. It follows that

$$\psi/\pi_1\pi\pi_1^{-1} = \psi;$$

and that is, $\pi_1\pi\pi_1^{-1}$ must be one of the permutations that leaves ψ unchanged, say k_i, a permutation of Q.

We accordingly have

$$\pi = \pi_1^{-1}k_i\pi_1.$$

If, reciprocally, π has this form, then is

$$\psi_1/\pi = \psi/\pi_1\pi = \psi/\pi_1\pi_1^{-1}k_i\pi_1 = \psi/k_i\pi_1 = \psi_1;$$

and that is, ψ_1 allows the permutation π.

It is thus shown that the group to which ψ_1 belongs may be indicated by the symbol

$$\pi_1^{-1}Q\pi_1.$$

That $\pi_1^{-1}Q\pi_1$ is in fact a group, is seen through compounding, say

$$\pi_1^{-1}k\pi_1\pi_1^{-1}k_1\pi_1 = \pi_1^{-1}kk_1\pi_1,$$

which permutation belongs to $\pi_1^{-1}Q\pi_1$.

The groups to which the conjugate quantities ψ, ψ_1, $\cdots$, ψ_{j-1} belong, namely,

$$Q,\ \pi_1^{-1}Q\pi_1,\ \pi_2^{-1}Q\pi_2,\ \cdots,\ \pi_{j-1}^{-1}Q\pi_{j-1} \tag{6}$$

may be called the *conjugate divisors of* P, or briefly, the *conjugate groups*. (See, for example, Netto, §§ 45–46.)

If the elements of two groups

$$Q = k,\ k_1,\ k_2,\ \cdots,$$
$$Q' = k',\ k_1',\ k_2',\ \cdots$$

are related to one another uniquely and in such a manner that k, k' and k_1, k_1', being two pairs of corresponding elements, their compounds kk_1, $k'k_1'$ are also corresponding elements, the two groups are said to be *isomorphic.* (See Art. 214, and Jordan, §§ 67–74.)

The manner of composition of the two permutations

$$\pi^{-1}k_i\pi\pi^{-1}k_h\pi = \pi^{-1}k_ik_h\pi$$

shows that all conjugate groups are isomorphic.

If π is an arbitrary permutation of P and therefore of the form $k\pi_r$, the group $\pi^{-1}Q\pi$ is always found among the conjugate groups (6), namely,

$$\pi_r^{-1}k^{-1}Qk\pi_r = \pi_r^{-1}Q\pi_r.$$

The derivation of $\pi^{-1}Q\pi$ from Q is sometimes called a

transformation of the group Q through π, and $\pi^{-1}Q\pi$ is called a group transformed out of Q.

ART. 221. **Reduction of the Galois Resolvent. Normal Divisors of a Group.** The question which is to be considered next is the gradual reduction of the group of a given equation. This can be done by adjoining certain algebraic quantities to the stock-realm.

As in the preceding article, let P be the Galois group of degree p and let Q be one of its divisors of degree q and of index j. Let $\psi = \psi(\alpha^{(0)}, \alpha^{(1)}, \cdots, \alpha^{(n-1)})$ be a function that permits the permutations Q, the conjugate quantities being

$$\psi, \psi_1, \cdots, \psi_{j-1}. \tag{1}$$

The following theorem may be proved:

THEOREM I. *The conjugate quantities (1) are the roots of an irreducible equation.*

For, let t be a variable and form the function

$$\varphi(t) = (t-\psi)(t-\psi_1)\cdots(t-\psi_{j-1}).$$

Observe that this function remains unchanged when it is subjected to any permutation of P and therefore (Art. 211, end) its coefficients must belong to $\mathfrak{R}$. To show that this function is irreducible, assume that it is factorable and let $\varphi_1(t)$ be one of its irreducible factors and assume also that $t=\psi$ is a root of $\varphi_1(t)$, so that $\varphi_1(\psi)=0$.

Since (Art. 214, Theorem I) all the permutations of P are applicable to this function, it is seen that φ_1 vanishes for all the quantities $\psi, \psi_1, \cdots, \psi_{j-1}$, and is therefore, neglecting a constant multiplicative factor, identical with φ.

The Lagrange Theorem: [1]

[1] Lagrange, "Reflexions sur la résolution algébrique des équations." *Oeuvres.* Tome III, § 100. Only a special case of this theorem was given by Lagrange, namely, the case in which the roots are independent variables; in its generality it was proved by Galois. See Jordan, §§ 60, 61.

THEOREM II. *Every quantity of the realm $\mathfrak{R}$ which permits the permutations of the group Q is contained in the realm $\mathfrak{R}(\psi)$, where ψ is a function that belongs to Q.*

Proof. Let ω be a function which permits the permutations of Q, and is a function which is changed into a function ω_i by each of the permutations of a sub-group $Q\pi_i (i=1,\ 2,\ \cdots,\ j-1)$. Thus, corresponding to the conjugate quantities

$$\psi,\ \psi_1,\ \cdots,\ \psi_{j-1}$$

there are the quantities

$$\omega,\ \omega_1,\ \cdots,\ \omega_{j-1},$$

which are not necessarily all different.

Form the function

$$\Phi(t)\left[\frac{\omega}{t-\psi}+\frac{\omega_1}{t-\psi_1}+\cdots+\frac{\omega_{j-1}}{t-\psi_{j-1}}\right]=F(t),$$

and observe that this function remains unchanged when to it are applied the permutations of P. Its coefficients are therefore quantities in $\mathfrak{R}$.

Writing $t=\psi$, it is seen that

$$\omega=\frac{F(\psi)}{\Phi'(\psi)},$$

as was to be proved.

EXAMPLE. **Prove that all functions that belong to the same group may be expressed rationally through any one of them.**

THEOREM III. *If the function ψ which permits the group Q is adjoined to the realm $\mathfrak{R}$, then in $\mathfrak{R}(\psi)$ the group P is reduced to Q.*

For, observe that due to Theorem I, Art. 214, every equation in $\mathfrak{R}$ among the quantities $\alpha,\ \alpha^{(1)},\ \cdots,\ \alpha^{(n-1)}$ is also satisfied when a permutation of P is applied to the equation.

And, further, note first that every equation in $\Re(\psi)$ that exists among the roots $\alpha, \alpha^{(1)}, \cdots, \alpha^{(n-1)}$ of the fundamental equation $F(x)=0$, permits the permutations of Q, since Q is contained in P and since ψ remains unchanged through the permutations of Q; and secondly, due to the Lagrange Theorem, every function which remains unchanged through Q belongs to $\Re(\psi)$.

These are the characteristic criteria of the Galois group in $\Re(\psi)$. (See Art. 214, Theorems I and II.)

The Theorem III may also be expressed as follows:

THEOREM III. *The normal realm* $\mathfrak{N}=\Re(\alpha, \alpha^{(1)}, \cdots, \alpha^{(n-1)})$ *is of the pth degree over* $\Re$ *and of the qth degree over* $\Re(\psi)$.

To the depression of the group through adjunction of ψ there corresponds, as has already been seen from the general fundamental theorems, a decomposition of the Galois resolvent.[1] For, let $g(t)=0$ be the Galois resolvent (Art. 210) and let ρ be one of its roots. Through the permutations $k, k_1, \cdots, k_{q-1}$ of Q, suppose that ρ becomes

$$\rho, \rho_1, \cdots, \rho_{q-1}, \tag{1}$$

where in general

$$\rho_h=\rho/k_h.$$

If to this system of quantities (1) there is applied a permutation of Q, Q being a group, it is evident that only the sequence of the quantities is changed. Hence, due to the Lagrange Theorem, the function

$$g(t, \psi)=(t-\rho)(t-\rho_1)\cdots(t-\rho_{q-1}) \tag{2}$$

is a function of the realm $\Re(\psi)$.

At the same time it is seen that $g(t, \psi)$ is a divisor of $g(t)$. Apply to ρ the permutations of the sub-group $\pi_i Q$ and that is, the permutations

$$\pi_i k, \pi_i k_1, \pi_i k_2, \cdots, \pi_i k_{q-1}.$$

[1] Cf. Dickson, *Modern Algebraic Theories*, pp. 174 et seq.

It is seen that ρ becomes

$$\rho_{0,i},\ \rho_{1,i},\ \cdots,\ \rho_{q-1,i} \qquad (i=1, 2, \cdots, j-1), \tag{3}$$

where

$$\rho_{h,i}=\rho/\pi_i k_h.$$

It is clear that any two of the series (3) are either identical or they have no element in common. For, if $\rho_{h,i}=\rho_{r,s}$, then is $\pi_i k_h=\pi_s k_r$, so that π_s is a permutation of the sub-group $\pi_i Q$. Further, the quantities (3) interchange only among themselves when to them is applied a permutation of Q. For $\pi_i Q k=\pi_i Q$, if k is a permutation of Q. Accordingly,

$$g_i(t, \psi)=(t-\rho_{0,i})(t-\rho_{1,i})\cdots(t-\rho_{q-1,i}) \qquad (i=1, 2, \cdots, j-1),$$

are functions of the realm $\Re(\psi)$; and it is seen, when ψ is adjoined to the realm $\Re$, that in the realm $\Re(\psi)$

$$g(t)=g(t, \psi)g_1(t, \psi)\cdots g_{j-1}(t, \psi). \tag{4}$$

Another method of decomposition of $g(t)$ into factors, although the factors are not all quantities of the realm $\Re(\psi)$ but are contained in the conjugate realms $\Re(\psi)$, $\Re(\psi_1)$, $\cdots$, $\Re(\psi_{j-1})$, respectively, is as follows: Write

$$\rho'_{h,i}=\rho_h/\pi_i=\rho/k_h\pi_i,$$

and observe that the quantities ρ, ρ_1, $\cdots\rho_{q-1}$ of the series (1) become through application of π_i

$$\rho'_{0,i},\ \rho'_{1,i},\ \cdots,\ \rho'_{q-1,i} \qquad (i=1, 2, \cdots, j-1). \tag{5}$$

Further, these quantities are changed only in sequence through a permutation of the group $\pi_i^{-1}Q\pi_i$, since $\rho'_{h,i}=\rho/k_h\pi_i$ becomes through application of $\pi_i^{-1}k_s\pi_i$,

$$\rho/k_h\pi_i\pi_i^{-1}k_s\pi_i=\rho/k_hk_s\pi_i.$$

Observe that the functions ψ_i permit the permutations of the groups

$$\pi_i^{-1}Q\pi_i \qquad (i=1, 2, \cdots, j-1).$$

As above, ψ through the application of π_i becomes ψ_i, while through the application of the same permutation

the functions

$$g(t, \psi_i) = (t - \rho'_{0,i})(t - \rho'_{1,i}) \cdots (t - \rho'_{a-1,i})$$

are had from the function given in formula (2). As these are all divisors of $g(t)$, and as the $j-1$ series as presented in (5) have no two elements in common, none of the functions $g(t, \psi_i)$ have a common factor. And from this it is seen that

$$g(t) = g(t, \psi)g(t, \psi_1) \cdots g(t, \psi_{j-1}) \tag{6}$$

offers a distribution into factors which in general is different from that in (4). The two distributions are coincident only when corresponding to a permutation π in P there can be found another permutation π' such that $\pi Q = Q\pi'$.

If Q and Q' are two different divisors of the group P, they may have in common certain permutations and always the identical permutation. If the identical permutation is the only permutation that the two groups Q and Q' have, they are said to be *prime* to each other. The collectivity (or complex) D of all permutations common to Q and Q' is called the *greatest common divisor* or *intersection* [1] of Q and Q'.

This D is always a group, for, if π and π' are two permutations common to Q and Q', then also $\pi\pi'$ is a permutation of both Q and Q' and therefore of D. This definition may be extended at once to several groups $Q, Q', Q'', \ldots$.

If ψ is a function that permits the permutations of Q, and if ψ' is a function that permits those of Q', then it is always possible (see Vol. I, Art. 50) to determine two rational numbers x and x' such that $\omega = x\psi + x'\psi'$ is a function that belongs to D. For, ω permits the permutations of D since both ψ and ψ' permit these permutations. If π is a permutation that does not belong to D,

[1] A word introduced in this connection by Study.

we cannot have simultaneously $\psi = \psi/\pi$ and $\psi' = \psi'/\pi$. Accordingly, we may so determine x and x' that ω is not equal to ω/π.

If then ψ and ψ' are simultaneously adjoined to the realm $\Re$, it is clear that the group P reduces to the group D (see Theorem III above).

The same process applied to several groups offers:

THEOREM IV. *If $Q, Q', Q'', \cdots$ are divisors of P, and if D is their intersection, while $\psi, \psi', \psi'', \cdots$ are functions that belong respectively to $Q, Q', Q'', \cdots$, the group P reduces to the group D if simultaneously adjunctions of $\psi, \psi', \psi'', \cdots$ are made to the stock-realm $\Re$.*

If we adjoin not only one root ψ of the auxiliary equation above $\varphi(t) = 0$, but all the roots $\psi, \psi_1, \cdots, \psi_{j-1}$ to the stock-realm, which therefore becomes $\Re(\psi, \psi_1, \cdots, \psi_{j-1})$, the group P is reduced to the group that is the intersection of all the groups that are conjugate with Q, so that D is here the greatest common divisor of all groups $\pi^{-1}Q\pi$ when π goes through all the permutations of P. (See Art. 221.)

Of peculiar interest is the case where all the conjugate groups $\pi^{-1}Q\pi$ are identical. In this case, due to the Lagrange Theorem, (above) the conjugate quantities $\psi, \psi_1, \cdots, \psi_{j-1}$, since they all permit the permutations of Q, are quantities of the realm $\Re(\psi)$ with the result that the realms $\Re(\psi)$, $\Re(\psi_1)$, $\cdots$, $\Re(\psi_{j-1})$ and $\Re(\psi, \psi_1, \cdots, \psi_{j-1})$ are identical; and that is, $\Re(\psi)$ is a normal realm above $\Re$. In this case the distribution into factors of $g(t)$ as presented in the formulas (4) and (6) are the same.

We call a divisor Q of P which has this property, a *normal divisor*, or an *invariantive sub-group*. Galois speaks of the *décomposition propre* of a group, meaning thereby the *eigentliche Theiler* as denoted by German authors.

Observe that if Q is a normal divisor of P, the adjunction of ψ to $\mathfrak{R}$ is of the same significance as if all the roots of the auxiliary equation were adjoined to $\mathfrak{R}$.

THEOREM V. *Even if Q is not a normal divisor of P, the greatest common divisor D of all conjugate divisors $\pi^{-1}Q\pi$ is a normal divisor of P.*

For, if k is a permutation of D and therefore of

$$Q,\ \pi_1^{-1}Q\pi_1,\ \pi_2^{-1}Q\pi_2,\ \cdots,\ \pi_{j-1}^{-1}Q\pi_{j-1},$$

the same is true of every permutation $\pi^{-1}k\pi$; and that is, $\pi^{-1}D\pi$ is a divisor of D and being of the same degree, must be equal to D.

A group which besides itself and the identical group contains no normal divisor is called a *simple group* (Vol. I, Art. 81). The intersection of all groups that are conjugate with a simple group is either the group itself or the identical group, according as the simple group is a normal divisor of P or not.

If Q is a normal divisor of P and if D is a normal divisor of Q, D is a divisor of P. If, however, D is a normal divisor of P and is also a divisor of Q, it is a normal divisor of Q.

ART. 222. **The Groups of the Resolvents.**[1] Let

$$\varphi(t) = (t-\psi)(t-\psi_1)\cdots(t-\psi_{j-1}).$$

If Q is the identical group, so that $q=1$ and $p=qj=j$, then $\varphi(t)$ is of the same degree as the Galois resolvent $g(t)$. Further, every quantity of $\mathfrak{N}$ permits the identical permutation. Hence, every quantity of $\mathfrak{N}$ including the roots $\alpha,\ \alpha^{(1)},\ \alpha^{(2)},\ \cdots,\ \alpha^{(n-1)}$ may be rationally expressed through ψ, thus making $\mathfrak{N}=\mathfrak{R}(\psi)$. It follows, in a more general sense, that the equations $\varphi(t)=0$ may be called *resolvent*.

Two cases are to be distinguished:

[1] Weber's *Algebra*, Vol. I, pp. 553 ff.

1. If the conjugate groups $\pi^{-1}Q\pi$ have no common divisor, the simultaneous adjunction of all the roots of the resolvent $\varphi(t)=0$ to the stock-realm has, due to Theorem IV of the preceding article, the same significance as the adjunction of a function which belongs to the unit group and accordingly, the solution of the given equation is coextensive with the solution of the resolvent.

We then have

$$\mathfrak{N}=\mathfrak{R}(\psi, \psi_1, \cdots, \psi_{j-1});$$

and a Galois resolvent of the equation $\varphi(t)=0$ is at the same time a Galois resolvent of the original equation. In this case $\varphi(t)=0$ is called a *total resolvent* of the given equation.

2. If the conjugate groups $\pi^{-1}Q\pi$ have a common divisor D that is different from the unit-group, and if D is of degree d, being from above a normal divisor of P, then the simultaneous adjunction to the stock-realm $\mathfrak{R}$ of all the functions that are conjugate to ψ, has the same significance as the adjunction of a quantity that belongs to D. Through this adjunction the Galois resolvent of the given equation is not solved completely but is distributed into factors, each of degree d. In this case $\varphi(t)$ is called a *partial resolvent*.

If P is a simple group, there exist only total resolvents; while if P has normal divisors, a partial resolvent may be found corresponding to each such normal divisor.

The same difference makes its appearance, if the Galois group of the resolvent $\varphi(t)$ is considered. It may be shown that this group consists of those changes which appear in the series of the quantities

$$\psi, \psi_1, \psi_2, \cdots, \psi_{j-1} \tag{1}$$

through application of all the permutations π of P. For, every equation in $\mathfrak{R}$ involving the quantities (1) remains

such, if to it any of the operations π is applied, since such a permutation π is applicable to the α's (Theorems I, II, III, of Art. 214) and therefore also to the ψ's; and if a function in $\mathfrak{R}$ of the quantities $\psi, \cdots, \psi_{j-1}$ permits all these permutations, it also permits all the permutations of P and is therefore a quantity of $\mathfrak{R}$.

The next problem is to determine the degree of this group. Among the permutations of P those permutations and only those will cause no changes among the quantities (1) which simultaneously appear in all the conjugate groups $\pi Q \pi$, and that is, in their greatest common divisor D. Let σ denote a permutation of D. If then π and π_1 cause the same permutation among the quantities (1), then $\pi_1 \pi^{-1}$ will bring about the initial arrangement among the ψ's. And, consequently

$$\pi_1 \pi^{-1} = \sigma \qquad \text{or} \qquad \pi_1 = \sigma \pi.$$

Thus, *all permutations of the sub-group $D\pi$ and only these, produce one and the same permutation among the quantities (1).* In other words, the degree of the Galois group of the resolvent $\varphi(t) = 0$ is equal to the number of these sub-groups, and that is, equal to the quotient p/d or to the index of the divisor D of P.

If D is the identical group, so that $d = 1$, and consequently, $\varphi = 0$ is a total resolvent, the degree of its group is as high as the degree of the resolvent of the original equation, both groups being isomorphic. In this case through the consideration of the group, nothing is won.

If, on the other hand, Q is a normal divisor and therefore D identical with Q, then is $\varphi(t) = 0$ a partial resolvent and the degree of its group is equal to the index j of the divisor Q of P. After the adjunction of a root of this resolvent to the original stock-realm, the group of the

original equation reduces to Q which is of degree q. Thus a splitting up of the resolvent is produced.

If resolvents of the smallest possible degree are desired, we must seek divisors of P which are of the highest possible degree and therefore of the smallest index. And if one wishes to bring about a reduction of the group, it is necessary to find a normal divisor of P.

ART. 223. **Reduction of the Galois Group through Adjunction of Arbitrary Irrationalities.** The solution of an algebraic equation is, according to the Galois conception, replaced through that of another equation. Through adjunction of well chosen algebraic quantities to the stock-realm is produced a factorization of the Galois resolvent.

The problem may be presented as follows: In the original stock-realm $\mathfrak{R}$ the Galois resolvent $g(t)=0$ is irreducible. The realm $\mathfrak{R}$ is extended to another realm $\mathfrak{R}(\epsilon)$, say, in which the resolvent is factorable. $\mathfrak{R}(\epsilon)$ is of course an algebraic realm and ϵ satisfies in $\mathfrak{R}$ an irreducible equation

$$\chi(\epsilon)=0. \tag{1}$$

We assume that in $\mathfrak{R}(\epsilon)$ the resolvent $g(t)$ is factorable, one of its irreducible factors being

$$g_1(t)=g_1(t,\ \epsilon), \tag{2}$$

which has the root $t=\rho$, where ρ is also a root of $g(t)=0$. Let the degree of $g_1(t,\ \epsilon)$ be q and let the roots of $g_1(t,\ \epsilon)=0$ be

$$\rho,\ \rho_1,\ \cdots,\ \rho_{q-1}, \tag{3}$$

so that

$$g_1(t,\ \epsilon)=(t-\rho)(t-\rho_1)\cdots(t-\rho_{q-1}). \tag{4}$$

First of all, it is to be proved that the following substitutions of P, namely, $(\rho,\ \rho)$, $(\rho,\ \rho_1)$, $\cdots$, $(\rho,\ \rho_{q-1})$ form a

group Q. To prove this, write as in Art. 211,

$$\rho_i = \Theta_i(\rho) \qquad (i=1, \cdots, q-1),$$

and observe that the equation

$$g_1[\Theta_i(t), \epsilon] = 0$$

has a root, namely, $t=\rho$ in common with $g_1(t)=0$. The equation $g_1(t)=0$ in $\Re(\epsilon)$ is irreducible. Hence $g_1[\Theta_i(t), \epsilon]$ is divisible by $g_1(t)$. It follows, if ρ_2 is one of the roots (3), that also

$$\Theta_1(\rho_2) = \rho_i$$

where ρ_i is one of the roots (3). As

$$\rho_1 = \Theta_1(\rho) \qquad \text{and} \qquad \rho_i = \Theta_1(\rho_2),$$

it is clear that

$$(\rho, \rho_2) = (\rho_1, \rho_i).$$

And since

$$(\rho, \rho_1)(\rho_1, \rho_i) = (\rho, \rho_i),$$

it is seen that (ρ, ρ_i) is compounded of (ρ, ρ_1) and (ρ, ρ_2), thus proving the group property of Q.

Denote the index of Q by j and put

$$p = jq. \tag{5}$$

The product (4) permits the substitutions of the group Q; and, if as above ψ is a function in $\Re$ which belongs to this group, then due to the Lagrange Theorem, the function $g_1(t, \epsilon)$ may be rationally expressed through ψ. And that is, $g_1(t, \epsilon)$ is a function of t in the realm $\Re(\psi)$ of the jth degree and accordingly may be denoted by $g(t, \psi)$.

The quantity ψ is the root of the auxiliary irreducible equation (Art. 221)

$$\varphi(u) = 0, \tag{6}$$

the other roots being $\psi_1, \psi_2, \cdots, \psi_{j-1}$.

It was seen in Art. 221 (6) that $g(t)$ could be distributed into the factors

$$g(t) = g(t, \psi)g(t, \psi_1) \cdots g(t, \psi_{j-1}). \tag{7}$$

Observe that by definition $g(t, \psi) = g_1(t, \epsilon)$ and that this equation is not true, if for ψ any of the quantities $\psi_1, \cdots, \psi_{j-1}$ is written; otherwise, there would be a double factor on the right of equation (7). Hence, it is possible to give a rational value to t such that the equations

$$g(t, u) - g_1(t, \epsilon) = 0 \qquad \text{and} \qquad \varphi(u) = 0$$

have *only one* root in common. Accordingly, the greatest common divisor of these equations expresses u rationally in ϵ; and if u is put $= \psi$ in the two equations, it follows that ψ is a rational function of ϵ.

The realm $\Re(\psi)$ is therefore a divisor of the realm $\Re(\epsilon)$. The degree of the realm $\Re(\epsilon)$ and that is, the degree of the irreducible equation $\chi(\epsilon) = 0$, is therefore (Vol. I, Art. 68) a multiple of j, where j is the degree of the irreducible equation that is satisfied by ψ. If the degree of the auxiliary equation $\varphi(u) = 0$ is j, which is the case if the degree of $\chi(\epsilon)$ is a prime integer, then ϵ and ψ being primitive quantities, the realms $\Re(\epsilon)$ and $\Re(\psi)$ are identical and ϵ can be rationally expressed through ψ, say $\epsilon = G(\psi)$. And if for ψ are written the other roots $\psi_1, \cdots, \psi_{j-1}$ of $\varphi(u) = 0$, we have the conjugate roots $\epsilon_1, \cdots, \epsilon_{j-1}$ of $\chi(\epsilon) = 0$.

It is evident that ϵ may be taken for ψ itself and we have a factorization in the form

$$g(t) = g(t, \epsilon) g(t, \epsilon_1) \cdots g(t, \epsilon_{j-1}).$$

Since ψ and its conjugates belong to the realm $\Re(\rho) = \Re$, it is seen that the quantities $\epsilon, \epsilon_1, \cdots, \epsilon_{j-1}$ all belong to this realm.

The above results are of extreme importance and should be particularly emphasized.

If $F(x) = 0$ is a given equation and if $\Re$ is the corresponding Galois realm, the quantities of $\Re$ were called by

Kronecker the *natural irrationalities* of the equation $F(x)=0$.

Accordingly, we have the following:

THEOREM. *Every possible reduction of the Galois group is effected through adjunction of a natural irrationality to the stock-realm. If j is the index of the reduced group with respect to the original group, and that is, the degree of the auxiliary equation which ψ satisfies, the reduction cannot be brought about through the adjunction of a realm of degree lower than j. The degree, however, may be equal to j and in that case, the adjoined irrationality is a natural one. If the degree of the adjoined realm is greater than j, it must be a multiple of j.* (See Jordan, pp. 261 ff.)

ART. 224. For future reference we may insert here certain observations regarding the divisors of any finite group. Let P be any finite group whose divisors are Q and R. Denote the elements of these groups respectively by a, b and c, where the b's and c's are found among the a's.

Denote the index of the divisor R of P by

$$j=(P, R),$$

so that, if

$$P=R+R_1+R_2+\cdots+R_k+\cdots+R_{j-1},$$

then is

(1) $$P=R+Ra_1+Ra_2+\cdots+Ra_k+\cdots+Ra_{j-1},$$

where $a_1, a_2, \cdots, a_{j-1}$ are elements of $R_1, R_2, \cdots, R_{j-1}$ respectively. (Weber, *Algebra*, Vol. II, p. 21.)

Consider next the complex

(2) $$Ra_kQ=P_k,$$

say; and observe that, if any element of a sub-group Ra is found in P_k, then P_k contains all the elements of Ra. For if a is any element of this complex and is consequently of the form $a=ca_kb$, then every element c_ia is of the same

form. To determine the number of sub-groups Ra_i that are found in P_k, let e be any element of Q that satisfies the condition

$$Ra_k = Ra_k e. \tag{3}$$

It follows that $a_k e$ is an element of Ra_k, so that $e = a_k^{-1} R a_k$. Hence the condition (3) is satisfied for all elements e of Q_k, where Q_k is the intersection of Q and $a_k^{-1} R a_k$. Next observe that two sub-groups $Ra_k b$ and $Ra_k b_1$ are equal only if $b_1 b^{-1}$ is an element in Q_k, and that is, if $b_1 = eb$. For, if $Ra_k b_1 = Ra_k b$, then is $a_k b_1$ an element of $Ra_k b$ or $b_1 b^{-1}$ is an element of $a_k^{-1} R a_k$.

Hence, if b in $Ra_k b$ goes over all the elements of Q, each of the sub-groups Ra appears an equal number of times, in case it *does* appear. And this number is the degree of Q_k. With this it is proved that *the number of sub-groups Ra, which are present in the complex P_k, is equal to the index (Q, Q_k); and the number of elements (the degree) of P_k is $r(Q, Q_k)$, where r is the degree of R.*

ART. 225. **Imprimitive Groups.**[1] We may next apply the general results of the preceding articles to groups of a special nature. First we shall consider the imprimitive groups. In Art. 216 it was seen, if $F(x) = 0$ is an irreducible equation of the nth degree with an imprimitive group, that n may be distributed into two factors r, s, such that the roots fall into s series of r terms, namely:

$$\begin{aligned} A &= \alpha, \ \alpha_1, \ \cdots, \ \alpha_{r-1}, \\ B &= \beta, \ \beta_1, \ \cdots, \ \beta_{r-1}, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ S &= \sigma, \ \sigma_1, \ \cdots, \ \sigma_{r-1}. \end{aligned} \tag{1}$$

It was also seen that through the permutations of the group P the quantities of the individual rows are not

[1] See Netto, §§ 64 et seq.

separated but are permuted among themselves, the rows being permuted among themselves.

Among the permutations of the Galois group P of $F(x)$ there are certain permutations whose complex may be denoted by Q and which leave the individual series A, $B, \cdots, S$ standing, the indices in each of these rows being permuted. These permutations form for themselves a group since the composition of any two of them do not effect a change of rows. This group Q is a normal divisor of P. For, if k is a permutation of P, then π may bring about an interchange of rows while k leaves these rows standing, producing only in them a permutation of indices, and π^{-1} returns them to their initial state, so that $\pi^{-1}k\pi$ is a permutation of Q no matter what is the permutation π of P.

The group Q is intransitive. Through the adjunction to the stock-realm of a function ψ, which belongs to Q, it is seen that not only the Galois resolvent is reducible but the same is also true of the function $F(x)$ itself, which is factorable into s factors of the rth degree, namely,

$$F(x) = F_\alpha(x, \psi)F_\beta(x, \psi)\cdots F_\sigma(x, \psi). \tag{2}$$

The roots of $f_\alpha(x, \psi) = 0$ are the quantities of the series A. The Galois group of this equation consists of all permutations which are brought about among the quantities $\alpha, \alpha_1, \cdots, \alpha_{r-1}$ through the permutations of Q.

For the product

$$F_\alpha(x) = (x-\alpha)(x-\alpha_1)\cdots(x-\alpha_{r-1})$$

permits the permutations of Q and may therefore be expressed rationally through ψ. In every rational equation in $\Re(\psi)$ among the quantities $\alpha, \alpha_1, \cdots, \alpha_{r-1}$ these quantities are permuted as is required by the group Q; and if a function of the α's permits these permutations, it is contained in $\Re(\psi)$.

If j is the index of the divisor Q of P, the quantity ψ is a root of a partial resolvent $\chi(u)=0$ of the jth degree which is a normal equation and therefore its own resolvent. Observe that Q is a normal divisor of P and consequently identical with the groups

$$Q,\ \pi_1^{-1}Q\pi_1,\ \pi_2^{-1}Q\pi_2,\ \cdots,\ \pi_{j-1}^{-1}Q\pi_{j-1}.$$

If the roots of the resolvent $\chi(u)=0$ are

$$\psi,\ \psi_1,\ \psi_2,\ \cdots,\ \psi_{j-1}, \tag{3}$$

the Galois group of this resolvent consists of the substitutions

$$(\psi,\ \psi),\ (\psi,\ \psi_1),\ \cdots,\ (\psi,\ \psi_{j-1}). \tag{4}$$

These are brought about through the permutations of the sub-groups

$$Q,\ Q\pi_1,\ \cdots,\ Q\pi_{j-1}. \tag{5}$$

Each permutation of a sub-group effects a certain permutation among the rows A, B, $\cdots$, S and these permutations are all different. For, if the same permutation were brought about among the rows by π_1 and π_2 then $\pi_2\pi_1^{-1}$ would be a permutation of Q. Hence, $Q\pi_2\pi_1^{-1}=Q$ or $Q\pi_2=Q\pi_1$, so that $Q\pi_2$ and $Q\pi_1$ would not be different.

It is thus seen that the permutation group of the partial resolvent $\chi(u)=0$ is isomorphic with the group of permutations which are caused through P among the rows A, B, $\cdots$, S.

If by Q_α we understand the complex of permutations of P through which the row A is not shoved into another row, then evidently Q_α is a group. If π_β is a permutation through which the row A is caused to become the row B, which permutation must exist on account of the presupposed transitivity of P, then $Q_\alpha\pi_\beta$ is a sub-group to Q_α through which A is transformed into B. If k is a permutation of Q_α then is the effect of the permutation of $k\pi_\beta$ upon α_i, which may be denoted by $\alpha_i/k\pi_\beta$, a change of

α_i to β_j, say; so that

$$\alpha_i/k\pi_\beta=\beta_j \qquad \text{or} \qquad \alpha_i=\beta_j/\pi_\beta^{-1}k^{-1}.$$

Further, on the one hand $\alpha_i/\pi_\beta=\beta_h$, say, and on the other hand

$$\alpha_i/\pi_\beta=\beta_j/\pi_\beta^{-1}k^{-1}\pi_\beta=\beta_h.$$

Thus the permutation $\pi_\beta^{-1}k^{-1}\pi_\beta$ changes one β to another β; and as k^{-1} is any permutation of the group Q_α, it is seen that the permutations of its conjugate group $\pi_\beta^{-1}Q_\alpha\pi_\beta=Q_\beta$ have the effect of permuting the β's in the row B.

In this manner we have the conjugate groups

$$Q_\alpha, Q_\beta, \cdots, Q_\sigma,$$

whose greatest common divisor is the normal group Q, considered above.

A function y_α which belongs to the group Q_α is the root of an equation of the sth degree in $\Re$. Let $\varphi(y)=0$ be this equation, the other roots of which are derived from y_α through application of permutations of the sub-groups

$$Q_\alpha\pi_\beta, Q_\alpha\pi_\gamma, \cdots, Q_\alpha\pi_\sigma.$$

And the equation $\chi(u)=0$ of degree j is the Galois resolvent of $\varphi(y)=0$. For the realm of rationality

$$\Re(y_\alpha, y_\beta, \cdots, y_\sigma) \text{ is } \Re(\psi),$$

where ψ is a quantity that belongs to Q and satisfies the equation $\chi(u)=0$ given above. It was seen that the group of the equation $\chi(u)=0$ of degree j is isomorphic with the group of permutations which caused the interchanging of the rows $A, B, \cdots, S$.

Due to the transitivity of P, these systems are transitively changed into one another and since the changes among $y_\alpha, y_\beta, \cdots, y_\sigma$ correspond to the changes of the rows $A, B, \cdots, S$, it is seen that $\varphi(y)$ is irreducible in $\Re$.

The simultaneous adjunction of all the roots of $\varphi(y)=0$ to the realm $\Re$ has the same effect as the adjunction of ψ;

namely, that of reducing the group of the equation $F(x)=0$ from P to Q.

Through the adjunction of y_α a rational factor $F(x, y_\alpha)$ is separated from $F(x)$ and the roots of $F(x, y_\alpha)$ are the quantities of the row A.

Through the adjunction of the other quantities $y_\beta, y_\gamma, \cdots, y_\sigma$ there arises the factorization

$$F(x)=F(x, y_\alpha)F(x, y_\beta)\cdots F(x, y_\sigma). \tag{6}$$

These functions $F(x, y_\alpha), \cdots, F(x, y_\sigma)$ coincide with the factors in (2), namely, $F_\alpha(x, \psi), F_\beta(x, \psi), \cdots, F_\sigma(x, \psi)$.

It may be remarked that the function $F(x, y_\alpha)$ is irreducible in the realm $\Re(y_\alpha)$. For, due to the assumed irreducibility of $F(x)=0$ in $\Re$, there are in P certain permutations through which α is transposed into any other α_i of the row A and these permutations belong to Q_α. Hence if a rational function $\varphi(x, y_\alpha)$ vanishes for $x=\alpha$, then every $\varphi(\alpha_i, y_\alpha)$ must be zero (Theorem I, Art. 214).

It follows that $\varphi(x, y_\alpha)$ must be divisible by $F(x, y_\alpha)$. It does not follow, however, that

$$F(x, y_\alpha)=F_\alpha(x, y_\psi)$$

is irreducible in the realm $\Re(\psi)$.

It is of interest to study the relations among the Galois groups of the factors $F(x, y_\alpha), \cdots, F(x, y_\sigma)$. It has been seen above that the group of the factor $F(x, y_\alpha)$ in the realm $\Re(\psi)$ are had if we seek all the permutations of the row A that are due to the permutations of Q. Denote this group of permutations by P_α and similarly let P_β denote the group of permutations of $F(x, y_\beta), \cdots$, while P_σ is the group of permutations of $F(x, y_\sigma)$.

From P take any $s-1$ permutations $\pi_\beta, \cdots, \pi_\sigma$ such that through π_β the row A becomes the row $B, \cdots$, through π_σ the row A becomes the row S. These results

may be indicated without the loss of generality by

$$\pi_\beta = \begin{pmatrix} \alpha_0, & \alpha_1, & \cdots, & \alpha_{r-1} \\ \beta_0, & \beta_1, & \cdots, & \beta_{r-1} \end{pmatrix}, \cdots, \pi_\sigma = \begin{pmatrix} \alpha_0, & \alpha_1, & \cdots, & \alpha_{r-1} \\ \sigma_0, & \sigma_1, & \cdots, & \sigma_{r-1} \end{pmatrix}.$$

Next let k be any permutation of Q which brings about a change among the α's, say

$$(\alpha) = \begin{pmatrix} \alpha_0, & \alpha_1, & \cdots, & \alpha_{r-1} \\ \alpha_{a_0}, & \alpha_{a_1}, & \cdots, & \alpha_{a_{r-1}} \end{pmatrix}.$$

Observe that $\pi_\beta^{-1} k \pi_\beta = k_\beta$, say, is a permutation of Q which causes among the β's the change

$$(\beta) = \begin{pmatrix} \beta_0, & \beta_1, & \cdots, & \beta_{r-1} \\ \beta_{a_0}, & \beta_{a_1}, & \cdots, & \beta_{a_{r-1}} \end{pmatrix},$$

and that is, the same changes among the indices of the β's as were effected through k among the indices of the α's. For, let k_β be a permutation of (β) and note that

$$k = \pi_\beta k_\beta \pi_\beta^{-1},$$

is a permutation of Q upon the β's that corresponds exactly with those that have been caused among the α's.

Note that Q is the group of permutations which changes the elements of the various rows in (1) without changing any of the rows.

With this is proved the following:

THEOREM I. *In the case of an irreducible imprimitive equation, the roots may be so arranged in the individual rows that the equations*

$$F(x, y_\alpha) = 0, \cdots, F(x, y_\sigma) = 0$$

all have the same group in the realm $\Re(\psi)$.

If the notation of the roots is not chosen in the manner indicated, the groups will be at least isomorphic.

It is seen that an imprimitive transitive group has an intransitive normal divisor.

The question is next asked: When has a transitive group an intransitive normal divisor? It will be proved

that such a group must be imprimitive. For, let P be a transitive group of permutations and Q an intransitive normal divisor of P. Further, suppose that

$$A = \alpha, \alpha_1, \cdots, \alpha_{r-1}$$

is one of the systems, whose elements through Q are changed only among one another in such a way however that the elements of A are transitively connected through Q. And that is, through the permutations of Q every element α is transposed into every other α.

If one of the permutations π of P changes the elements of A into the elements

$$B = \beta, \beta_1, \cdots, \beta_{r-1},$$

then these elements are either all identical with the α's or they are all different from them. For, through the group $\pi^{-1}Q\pi$, which by hypothesis is identical with Q, the β's are only transposed among themselves and transitively as the α's. Were only a part of the α's appearing in B due to the permutation π, then, contrary to the assumption, these would be changed into other elements that did not appear in A.

If there exist other elements than those expressed through A, to which the permutations of P are applicable, there also exists, since P is transitive, a permutation π through which A is transposed into an entirely different system B. If k is a permutation of Q, then through the permutation $\pi^{-1}k\pi$, which also is a permutation of Q, the same change is brought about among the indices β of the row B as the permutation k caused among the indices of the α's. From this it follows that through Q the β's also are only permuted among one another. If with A and B all the elements are not reached, we may form in the same way a third system C which exists through the permutation π' operating on the α's and

through $\pi^{-1}\pi'$ operating on the β's. The system C has in common no element with either A or B. The process may be continued until all the elements are included and with this we come to the following:

THEOREM II. *A transitive group only when it is imprimitive, has an intransitive normal divisor which is different from the identical group. The systems of intransitivity of the normal divisor are systems of imprimitivity of the given group.*

A third theorem relative to equations is as follows, when application is made of Theorems I and II above:

THEOREM III. *An irreducible equation $F(x)=0$ in $\mathfrak{R}$, if it becomes reducible through the adjunction to $\mathfrak{R}$ of all the roots of a resolvent, may be decomposed into several irreducible factors of equal degree and of equal group.*

It follows that if an irreducible primitive equation is reduced through the adjunction of the roots of a resolvent, it is decomposed into linear factors and that is, it is completely solved.

This is always the case if the degree of the equation $F(x)=0$ is a prime number, since such an equation cannot be imprimitive.

A list of further results with numerous references may be found in Dickson's *Modern Algebraic Theories*, pp. 176 et seq.

ART. 226. **Abelian Equations.**[1] The degree of a transitive permutation group of m ciphers is always divisible by m and therefore is never less than m. For, if P is such a group and if Q_0 is the complex of the permutations of P which leave the cipher 0 unchanged, then is Q_0 also a

[1] See Kronecker, *Berliner Monatsbericht*, June, 1853; Feb., 1873; Mar., 1879; *Grundzüge*, § 1; *Works*, Vol. IV, pp. 1 et seq.; Weber, "Theorie der abelschen Zahlkörper," *Acta Math.*, Vols. 8 and 9; Netto, §§ 17 et seq.; Serret, §§ 532, 533; Jordan, §§ 400, 401; Weber, *Algebra*, Vol. I, p. 575.

group. On account of the assumed transitivity of P there is a permutation π_1 which changes 0 to 1, similarly, a permutation π_2 through which 0 becomes 2, $\cdots$, and a permutation π_{m-1} which changes 0 to $m-1$.

Observe that $Q_0\pi_i$ is the system of all the permutations of P which change 0 to i and accordingly

$$P = Q_0 + Q_0\pi_1 + \cdots + Q_0\pi_{m-1}. \tag{1}$$

From this it is seen that the degree of P is equal to the product of m by the degree of Q_0.

It follows that *the Galois group of an irreducible equation is never of lower degree than the degree of the equation.*

We have defined (Art. 210) a normal Galois equation by requiring that it be irreducible and that each of its roots may be rationally expressed in terms of any other root. From this it is seen that the group of a normal equation must reduce to the identical group if one of its roots is adjoined to the given stock-realm; and reciprocally, an equation which has this property, if it is irreducible, is always a normal equation.

Further, since the root α_0 belongs to the group Q_0, it follows from Theorem III, Art. 221, that if α_0 is adjoined to the stock-realm, that the group P reduces to the group Q_0; and if α_1 is adjoined to the stock-realm, P reduces to the group $\pi_1^{-1}Q_0\pi_1$, which group leaves undisturbed the cipher 1, etc. Hence, if P is to be the group of a normal equation, it is necessary and sufficient that Q_0 be the unit group, and consequently that $\pi = 1, \pi_1, \pi_2, \cdots, \pi_{m-1}$ constitute the group P.

With this is proved the following:

THEOREM. *In order that an irreducible equation be a normal equation, it is necessary and sufficient that the degree of the group be the same as that of the equation.*

We may next consider the general type of equation which was solved by Abel [1] and which are called the *Abelian equations.*

An equation of the mth degree $F(x)=0$ *with roots* $\alpha, \alpha_1, \cdots, \alpha_{m-1}$ *is said to be an Abelian equation, if each root may be rationally expressed through one of them, say* α *in the form*

$$(2) \qquad \alpha_1=\Theta_1(\alpha),\ \alpha_2=\Theta_2(\alpha),\ \cdots,\ \alpha_{m-1}=\Theta_{m-1}(\alpha),$$

and if further the condition

$$(3) \qquad \Theta_h\Theta_k(\alpha)=\Theta_k\Theta_h(\alpha)$$

is satisfied for every two of these functions.

In the above formula the expression $\Theta_h\Theta_k(\alpha)$ means that the function $\Theta_h(x)$ is to be formed for the argument $x=\Theta_k(\alpha)$. If $\mathfrak{R}$ is the stock-realm, it is seen that among the Abelian equations are to be found those through which the roots of unity are determined. For, if ρ is a primitive root of the equation $x^m-1=0$, for example, then every mth root is of the form $\rho^h=\Theta_h(\rho)$ and consequently

$$\Theta_k\Theta_h(\rho)=\Theta_k(\rho^h)=\rho^{hk}=\Theta_h\Theta_k(\rho).$$

Similarly, if ρ is added to the stock realm $\mathfrak{R}$, the equation

$$x^m-a=0$$

is an Abelian equation. For, if α is a root of this equation, then all the roots are of the form

$$\alpha_h=\rho^h\alpha.$$

Hence,

$$\Theta_h(x)=\rho^h x,$$

and consequently

$$\Theta_k\Theta_h(x)=\Theta_h\Theta_k(x)=\rho^{h+k}x.$$

Returning to the general theory, if the function $F(x)$ is not irreducible, it has a definite irreducible factor $\varphi(x)$,

[1] *Oeuvres complètes*, 1881, Vol. I, p. 418; see also Serret, §§ 529 et seq.; Jordan, §§ 400 et seq.

which has the root α and among the roots of $\varphi(x)=0$, there exist also the relations that are expressed through (2) and (3) above. Hence, $\varphi(x)=0$ is the Galois resolvent of $F(x)$ as set forth in Art. 210; and if $\varphi(x)=0$ is solved, then the roots of $F(x)=0$ are known. It is therefore sufficient, if we limit the discussion to irreducible Abelian equations.

The Galois group of an Abelian equation, whether it be reducible or irreducible, provided its roots are different from one another, has the property that the commutative law holds in the case of the composition of its permutations, and that is, the group is a *commutative group*. For, let

$$\alpha,\ \alpha_1=\Theta_1(\alpha),\ \cdots,\ \alpha_{m-1}=\Theta_{m-1}(\alpha) \tag{4}$$

be the roots of $F(x)=0$, and let

$$\alpha,\ \alpha'=\Theta'(\alpha),\ \alpha''=\Theta''(\alpha),\ \cdots \tag{5}$$

be the roots of the irreducible factor $\varphi(x)$ of $F(x)$. As seen above $\varphi(x)$ being a Galois resolvent, the group of the equation consists of the substitutions of the realm $\Re(\alpha)$, and that is, of the substitutions

$$\sigma=(\alpha,\ \alpha),\ \sigma'=(\alpha,\ \alpha'),\ \sigma''=(\alpha,\ \alpha''),\ \cdots. \tag{6}$$

This group however requires the commutative principle. For, let

$$\sigma'=(\alpha,\ \alpha')=[\alpha,\ \Theta'(\alpha)],$$
$$\sigma''=(\alpha,\ \alpha'')=[\alpha,\ \Theta''(\alpha)],$$

so that (Art. 212)

$$\sigma'\sigma''=[\alpha,\ \Theta'(\alpha)][\Theta'(\alpha),\ \Theta'\Theta''(\alpha)]=[\alpha,\ \Theta'\Theta''(\alpha)],$$

and

$$\sigma''\sigma'=[\alpha,\ \Theta''(\alpha)][\Theta''(\alpha),\ \Theta''\Theta'(\alpha)]=[\alpha,\ \Theta''\Theta'(\alpha)].$$

Since

$$\Theta'\Theta''(\alpha)=\Theta''\Theta'(\alpha),$$

it follows that

$$\sigma'\sigma''=\sigma''\sigma',$$

where σ' and σ'' are any two of the substitutions σ. It follows that the group of the substitutions of the realm $\Re(\alpha)$ and with it also the isomorphic group of permutations of $F(x)=0$ is *commutative.*

The inverse of this statement is also true, if the irreducibility is presupposed, and that is:

THEOREM. *An irreducible equation $\varphi(x)=0$ with commutative group is an Abelian equation.*

For, let $\alpha, \alpha_1, \cdots, \alpha_{m-1}$ be the roots of $\varphi(x)=0$, and let P be the group of this equation, which on account of the irreducibility of $\varphi(x)$ is transitive, and which by hypothesis is commutative. Let Q be the divisor of P which leaves undisturbed the cipher 0. If π_i is a permutation which changes 0 to i, then is $\pi_i^{-1}Q\pi_i$ the group of permutations in P which leave undisturbed the cipher i.

Since, however, in every composition of permutations of P the permutations may be interchanged, it is seen that

$$\pi_i^{-1}Q\pi_i=\pi_i^{-1}\pi_iQ=Q,$$

and that is, the group Q also leaves i unchanged. Due to the transitivity of P, it is seen that i may denote any of the ciphers $1, 2, \cdots, m-1$, so that Q is the identical permutation. It follows also that excepting the identical permutation there is no permutation which leaves unchanged a cipher. If, however, we adjoin one of the roots α to the stock-realm, the group P reduces to the group which leaves α unchanged, and that is, to the identical group. In this case the equation is solved and that is, each root of $\varphi(x)$ may be expressed rationally in terms of α. When this is true, $\varphi(x)=0$ is a normal equation and consequently its only Galois resolvent.

If $\alpha_k=\Theta_k(\alpha)$, then the Galois group of this equation consists of the substitutions

$$\sigma_k=[\alpha,\ \Theta_k(\alpha)];$$

and it follows that

$$\sigma_h\sigma_k=[\alpha,\ \Theta_h\Theta_k(\alpha)] \qquad \text{and} \qquad \sigma_k\sigma_h=[\alpha,\ \Theta_k\Theta_h(\alpha)].$$

Due to the presupposed commutative property of the substitutions, namely

$$\sigma_h\sigma_k=\sigma_k\sigma_h,$$

it follows that

$$\Theta_h\Theta_k(\alpha)=\Theta_k\Theta_h(\alpha);$$

and that is, $\varphi(x)=0$ is an Abelian equation. This is the reason that the commutative group is also called the Abelian group (Art. 213).

It follows further due to the theorems that were proved at the beginning of this article relative to the group of a normal equation, that in the case of a transitive Abelian permutation group, the number of permutations is the same as the number of ciphers that are permuted. (Weber's *Algebra*, Vol. I, p. 578.)

We have assumed in the above discussion that the equation $F(x)=0$ was irreducible. If we assume that any equation $F(x)=0$ has a commutative group P; and if $\varphi(x)$ is an irreducible factor of $F(x)$, the group P' of the equation $\varphi(x)=0$ is had, if the permutations of P are applied to the roots of $\varphi(x)=0$. If P is commutative, P' is also commutative.

From this follows the theorem:

THEOREM. *If a reducible equation $F(x)=0$ has a commutative group, then every irreducible divisor φ of F offers an Abelian equation $\varphi=0$.*

However, it is not necessary that the roots of one divisor φ be rationally expressible through the roots of another divisor of $F(x)=0$. Hence with reference to our definition, the equation $F(x)=0$ cannot always be designated as Abelian.

Finally, it is to be noted that in the case of a commutative group every divisor is normal since we always have

$$\pi^{-1}k\pi = k,$$

where π and k are arbitrary elements of a commutative group. In this connection read the chapter on Abelian groups by Jordan, *Traité des substitutions*, pp. 171–189.

ART. 227. **Reduction of Abelian Equations to Cyclic Equations.** It has been seen in the case of a transitive Abelian group that besides the identical permutation there is no permutation that leaves one cipher unchanged. From this follows another theorem. Suppose that π is a permutation of an Abelian group and let π be distributed into its cycles. Suppose that the cycle which contains the smallest number of ciphers is one of r ciphers. Then π^r leaves the ciphers in this cycle unchanged, and as the identical permutation is the only one that has this property, it follows that π^r must be the identical permutation. It also follows that all the remaining cycles of π, if such there are, must also consist of r elements with the result:

THEOREM I. *A permutation of a transitive Abelian group contains only cycles of equal number of ciphers.*

The number r of the terms of the cycle must be a divisor of m, if m is the degree of the group; and if $m = r \cdot s$, then is s the number of the cycles which constitute π.

If P is the group of an Abelian equation $F(x) = 0$ and if π is any permutation of P, that is not the identical permutation, then π may be distributed into its cycles

$$\pi = \gamma\gamma_1 \cdots \gamma_{s-1}, \tag{1}$$

where each cycle γ consists of r roots of the equation $F(x) = 0$.

These roots may be so arranged that

$$(2)\qquad \begin{cases} \gamma=(\alpha,\ \alpha_1,\ \cdots,\ \alpha_{r-1}), \\ \gamma_1=(\beta,\ \beta_1,\ \cdots,\ \beta_{r-1}), \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \gamma_{s-1}=(\sigma,\ \sigma_1,\ \cdots,\ \sigma_{r-1}). \end{cases}$$

If π is any permutation of P, then due to the commutative law for this group we have

$$(3)\qquad \pi_1^{-1}\pi\pi_1=\pi.$$

It follows, due to the method by which the permutation $\pi_1^{-1}\pi\pi_1$ is formed (Art. 218, Theorem IV) that π is not changed when π_1 is applied to the cycles which constitute π. Since, however, the cycles are completely determined, neglecting their sequence and the initial elements, it is seen that through application of any permutation π_1 of P, the elements of any cycle γ are not separated but are only changed cyclically among one another, and further the cycles may be interchanged. If then $s>1$, the group is *imprimitive*.

A rational function of the elements $\alpha,\ \alpha_1,\ \cdots,\ \alpha_{r-1}$, which does not change its value when the α's are subjected to the cyclic permutation γ, and to powers of this permutation, is called a *cyclic function* of the α's.

Denote such a function by

$$(4)\qquad \omega=\psi(\alpha,\ \alpha_1,\ \cdots,\ \alpha_{r-1}),$$

and let its conjugate values be

$$(5)\qquad \begin{cases} \omega_1=\psi(\beta,\ \beta_1,\ \cdots,\ \beta_{r-1}), \\ \cdot\qquad\cdot \\ \cdot\qquad\cdot \\ \cdot\qquad\cdot \\ \omega_{s-1}=\psi(\sigma,\ \sigma_1,\ \cdots,\ \sigma_{r-1}). \end{cases}$$

These quantities (Art. 225) are the roots of an irreducible equation

$$\Phi(t)=0,$$

whose group is had, when the permutations of P are applied to

(6) $$\omega, \omega_1, \cdots, \omega_{s-1}.$$

Observe that the change that is brought about among the quantities (6) by the permutation $\pi_1\pi_2$ is the same as if π_1 and π_2 separately had been applied to these quantities. The group of the permutations of (6) is therefore also commutative, and that is, $\Phi(t)=0$ is an Abelian equation of degree s.

If ω is adjoined to the stock-realm, then $F(x)$ may be decomposed into s factors each of the rth degree; and since ω_1 is a rational function of ω as is also $\omega_2, \cdots, \omega_{s-1}$, it follows that

$$F(x)=F_1(x, \omega)F_1(x, \omega_1), \cdots F_1(x, \omega_{s-1}),$$

where $F_1(x, \omega)$, say, has the roots $\alpha, \alpha_1, \cdots, \alpha_{r-1}$. The group of $F_1(x, \omega)$ consists only of the period of the cyclic permutation γ.

An equation whose group consists of a single cycle with the powers of the same is called a *cyclic equation.* It follows that the cyclic equations are the simplest special case of the Abelian equations. Accordingly, it has been proved that the solution of every Abelian equation may be made to depend upon the solution of an Abelian equation of lower degree and upon the solution of a series of cyclic equations. The theorem may then again be applied to the auxiliary equation $\Phi(t)=0$ of the sth degree and the process continued until we come to an auxiliary equation of the first degree. This gives rise to the result:

The solution of an Abelian equation may be reduced to that of a series of cyclic equations whose degrees are divisors of the degree of the given equation. (Cf. Jordan, § 405.)

In the definition of the cyclic equations it is not necessary to assume that they are irreducible. In general such equations may be defined as follows:

An equation of the mth degree $F(x)=0$ *with* m *different roots is called a* cyclic *equation in* $\Re$, *if its roots* $\alpha, \alpha_1, \cdots, \alpha_{m-1}$ *are not rational and if they may be so arranged that the cyclic functions of the roots are rational in* $\Re$.

And that is, if

$$\pi=(\alpha, \alpha_1, \cdots, \alpha_{m-1}) \tag{7}$$

is a cyclic permutation of the roots, then every function $\varphi(\alpha, \alpha_1, \cdots, \alpha_{m-1})$ which permits the permutations of the cyclic group

$$C=1, \pi, \pi^2, \cdots, \pi^{m-1} \tag{8}$$

must be rational in $\Re$.

The Galois group of a cyclic equation is either the period C itself, in which case the equation is irreducible, or the Galois group is a divisor of C. In this case if e and f are the two divisors of m and if

$$m=ef,$$

the group consists of the permutations

$$C_e=1, \pi^e, \pi^{2e}, \cdots, \pi^{(f-1)e}, \tag{9}$$

and the cyclic equation falls into e factors of the fth degree. For, if $\psi(\alpha, \alpha_1, \cdots, \alpha_{m-1})$ is a function which belongs to the group C, then by hypothesis it is a quantity of $\Re$, say a, so that

$$\psi(\alpha, \alpha_1, \cdots, \alpha_{m-1})=a.$$

No permutation that is not in C is applicable to ψ and consequently the group of the equation $F(x)=0$ can have no other substitutions than those that appear in C. If then π appears in the group of the equation, then is π identical with C; and, since C is transitive, the equation is

irreducible. But if π^e is the lowest power of π that appears in the group of the equation, then C_e is this group and since C_e is intransitive, if $e>1$, the equation is reducible.

The cyclic equations like all Abelian equations have the property that each root may be rationally expressed through any other. If $\alpha, \alpha_1, \cdots, \alpha_{m-1}$ are the roots of the cyclic equation $F(x)=0$, then is the function

$$F(x)\left(\frac{\alpha_1}{x-\alpha}+\frac{\alpha_2}{x-\alpha_1}+\cdots+\frac{\alpha}{x-\alpha_{m-1}}\right)=\Psi(x)$$

unchanged through the permutation π and consequently $\Psi(x)$ is a function of $\Re$.

Writing

$$\frac{\Psi(x)}{F'(x)}=\Theta(x),$$

it is seen that

$$(10)\quad \alpha_1=\Theta(\alpha),\ \alpha_2=\Theta(\alpha_1),\ \cdots,\ \alpha_{m-1}=\Theta(\alpha_{m-2}),\ \alpha=\Theta(\alpha_{m-1});$$

and this is true whether $F(x)$ is irreducible or not, provided $F(x)$ and $F'(x)$ have no root in common.

If the degree of the cyclic equation is not a prime integer, it may be further reduced after the method given above for the Abelian equations. (See Serret, §§ 535 et seq.) For, if $m=ef$ is any factorization of m into two factors, the permutation π^e may be distributed into e cycles γ of f terms, namely,

$$(11)\quad \begin{cases} \gamma=(\alpha, \alpha_e, \alpha_{2e}, \cdots, \alpha_{(f-1)e}), \\ \gamma_1=(\alpha_1, \alpha_{e+1}, \cdots, \alpha_{(f-1)e+1}), \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \gamma_{e-1}=(\alpha_{e-1}, \alpha_{2e-1}, \cdots, \alpha_{m-1}). \end{cases}$$

We may next determine a function ψ which belongs to

the first of these cycles, and write

$$(12)\qquad \begin{cases} \eta=\psi(\alpha,\ \alpha_e,\ \cdots,\ \alpha_{(f-1)e}), \\ \eta_1=\psi(\alpha_1,\ \alpha_{e+1},\ \cdots,\ \alpha_{(f-1)e+1}), \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \eta_{e-1}=\psi(\alpha_{e-1},\ \alpha_{2e-1},\ \cdots,\ \alpha_m). \end{cases}$$

These functions are all different from one another. They remain unchanged if their arguments are permuted cyclically. Through application of the permutation π the quantities $\eta,\ \eta_1,\ \eta_2,\ \cdots,\ \eta_{e-1}$ are cyclically changed into one another, and by hypothesis the cyclic functions of these quantities and therefore also their symmetric functions are rational.

They are therefore the roots of an equation of the eth degree, and $F(x)$ may be decomposed into e factors of the fth degree

$$F(x)=F(x,\ \eta)F(x,\ \eta_1),\ \cdots F(x,\ \eta_{e-1}),$$

each of which factors offers a cyclic equation of the fth degree for the roots of one of the cycles (11). For, write

$$F_1=(x-\alpha)(x-\alpha_e)\cdots(x-\alpha_{(f-1)e}).$$

It is evident that F_1 permits the permutations of the period of γ. Hence, F_1 permits also the same permutations as the function η, and accordingly by the Lagrange Theorem F_1 is a rational function of η, so that $F_1=F(x,\ \eta)$. The equation $F(x,\ \eta)=0$ is thus cyclic in $\Re(\eta)$, since the cyclic function of the roots of $F(x,\ \eta)=0$ belong to this realm.

Thus it has been shown that the solution of the cyclic equation of the mth degree is reduced to the solution of cyclic equations whose degrees are the prime factors of m. If for example m is a power of 2, then the solution is effected through the solution of a series of quadratics.

In this way Gauss (*Disquisitiones arithmeticae*, § VII), treated the problem of the division of the circle.

The following remark is of importance for what follows: The conception of the *normal equation* and the cyclic equation is the same if the degree is a prime number. For, if a cyclic equation is of a degree that is a prime integer, since it is irreducible, it is a normal equation. Reciprocally, let n, the degree of a normal equation, be a prime integer and observe that n is also the degree of the group of this equation.

If π is any permutation of this group then the degree of π, since it must be a divisor of n is equal to n and the group of the equation is $1, \pi, \pi^2, \cdots, \pi^{n-1}$ and therefore cyclic.

CHAPTER XIV

RELATIONS OF A REALM TO ITS DIVISORS

ART. **228. Relative Norms.** We may next consider the modifications which must be made in the definitions and theorems regarding algebraic numbers when, instead of the realm of rational numbers, any arbitrary algebraic realm is taken as the stock-realm. It is clear that certain important extensions must be made for the general theory of prime factors.[1]

Let α satisfy an irreducible algebraic equation of the mth degree

$$x^m + a_1 x^{m-1} + \cdots + a_m = 0,$$

where the a's are rational numbers, and that is numbers of the realm $\mathfrak{R}$. Further let Θ satisfy an irreducible equation of the nth degree

$$f(\Theta) = \Theta^n + \alpha_1 \Theta^{n-1} + \cdots + \alpha_n = 0, \tag{1}$$

where $\alpha_1, \alpha_2, \cdots, \alpha_n$ are numbers of the realm $\mathfrak{k} = \mathfrak{R}(\alpha)$. The realm $\mathfrak{R}(\alpha, \Theta)$ is an algebraic realm *above* $\mathfrak{R}(\alpha)$, which with respect to the realm $\mathfrak{R}(\alpha)$ is of the nth degree. (See Art. 189.)

In the absolute realm R the realm $\mathfrak{R}(\alpha, \Theta)$ is of the degree mn, and if τ is a primitive quantity in $\mathfrak{R}(\alpha)$, a basis of $\mathfrak{K} = \mathfrak{R}(\alpha, \Theta)$ is

$$\Theta^i \tau^h \quad (i = 0, 1, \cdots, n-1; h = 0, 1, \cdots, m-1). \tag{2}$$

For, due to the fact that (1) is irreducible, there can be no

[1] Dedekind, "Ueber die Discriminanten endlicher Körper," *Abh. der Gött. Ges. der Wissenschaften*, 1882; "Zur Theorie der Ideale," *Gött. Nachrichten*, 1894, Nr. 4. Hilbert, *Grundzüge*, etc.; *Gött. Nach.*, 1894, Nr. 3. See also Weber, *Algebra*, Vol. II, pp. 643 ff.

linear relation with rational coefficients among the mn quantities (2).

Every number Ω of the realm $\mathfrak{R} = \mathfrak{R}(\alpha, \Theta)$ is an integral function of the $n-1$st degree in Θ, whose coefficients belong to $\mathfrak{R}(\alpha)$; and any such number Θ satisfies in $\mathfrak{R}(\alpha)$ an irreducible algebraic equation of degree at most n. Ω is an algebraic *integer* in $\mathfrak{R}(\alpha)$ if 1 is the coefficient of the highest power, while the other coefficients of this equation are integers in $R(\alpha)$.

The complex of all integers in $\mathfrak{R}(\alpha, \Theta)$ may be denoted by $\mathfrak{O}$.

If $\Theta_1, \Theta_2, \cdots, \Theta_n$ are the roots of (1), the realms

$$\mathfrak{R}(\alpha, \Theta_1), \mathfrak{R}(\alpha, \Theta_2), \cdots, \mathfrak{R}(\alpha, \Theta_n) \tag{3}$$

are *conjugate* with *respect* to $\mathfrak{R}(\alpha)$.

If Ω is a number of $\mathfrak{R}$, it is a rational function of α and Θ; and if for Θ are written its conjugate values, we have n conjugate numbers $\Omega_1, \Omega_2, \cdots, \Omega_n$ in these n realms. Their product

$$\mathfrak{N}_\mathfrak{r}(\Omega) = \Omega_1\Omega_2 \cdots \Omega_n \tag{4}$$

is called the *relative norm* with respect to $\mathfrak{r} = \mathfrak{R}(\alpha)$ of the number Ω.

Observe that if η is any number of $\mathfrak{R}(\alpha)$, its norm $N_\mathfrak{r}(\eta)$ is a rational number.

The relative norm $\mathfrak{N}_\mathfrak{r}(\Omega)$ is a number in $\mathfrak{R}(\alpha)$ like η; and, if we take its norm in $\mathfrak{R}(\alpha)$, we have the *total norm* of Ω, namely

$$N_\mathfrak{r}(\Omega) = N_\mathfrak{r}\mathfrak{N}_\mathfrak{r}(\Omega), \tag{5}$$

which is a rational number.

In Art. 70 it was seen, if

$$F = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_m u_m,$$

where $u_1, u_2, \cdots, u_m$ are indeterminant quantities, that

$$FF' \cdots F^{(m-1)} = N(\mathfrak{a}),$$

where $\mathfrak{a}=(\alpha_1, \alpha_2, \cdots, \alpha_m)$. Similarly, if

$$\mathfrak{J}=[A_1, A_2, \cdots, A_n],$$

where the A's are capital alphas and are integers in $\mathfrak{K}$, it is seen that

$$\mathfrak{N}_\mathfrak{k}(\mathfrak{J})=\mathfrak{J}\cdot\mathfrak{J}'\cdots\mathfrak{J}^{(n-1)}=(A_1U_1+A_2U_2+\cdots+A_nU_n)$$
$$\times(A'U_1+\cdots+A'_nU_n)\cdots(A_1^{(n-1)}U_1+\cdots+A_n^{(n-1)}U_n)$$

is an ideal in $\mathfrak{k}$; that is, the partial norm of an ideal in $\mathfrak{K}$ is an ideal in $\mathfrak{k}$.

Similarly if by $\mathfrak{S}$ we denote the *spur* of a number in $\mathfrak{K}$ then

$$\mathfrak{S}_\mathfrak{k}(\Omega)=\Omega_1+\Omega_2+\cdots+\Omega_n \tag{6}$$

is the partial spur (or relative spur) of Ω in $\mathfrak{k}$. This sum is an integer in $\mathfrak{k}$, if Ω is an integer in $\mathfrak{K}$; while the *total spur* is

$$S_\mathfrak{k}(\Omega)=S_\mathfrak{k}\mathfrak{S}_\mathfrak{k}(\Omega). \tag{7}$$

If $\mathfrak{P}$ is a prime ideal in $\mathfrak{K}$, there is one and only one natural prime integer p that is divisible by $\mathfrak{P}$. If p is decomposed into its prime factors in $\mathfrak{k}$, one of these prime factors which may be denoted by $\mathfrak{p}$ is divisible by $\mathfrak{P}$. If $\mathfrak{a}$ is any ideal in $\mathfrak{k}$, which is divisible by $\mathfrak{P}$, then the greatest common divisor of $\mathfrak{p}$ and $\mathfrak{a}$, which is an ideal in $\mathfrak{k}$, is divisible by $\mathfrak{P}$, and is *not* a unit. Hence $\mathfrak{p}$ and $\mathfrak{a}$ are not relatively prime and hence $\mathfrak{a}$ is divisible by $\mathfrak{p}$, as $\mathfrak{p}$ has no other divisor save itself and units. If $\mathfrak{a}$ is also a prime ideal, then $\mathfrak{a}$ and $\mathfrak{p}$ are identical.

With this is proved the theorem:

THEOREM I. *If $\mathfrak{P}$ is a prime ideal in $\mathfrak{K}$, there is one and only one prime ideal $\mathfrak{p}$ in $\mathfrak{k}$ which is divisible by $\mathfrak{P}$, and every ideal in $\mathfrak{k}$ which is divisible by $\mathfrak{P}$ is at the same time divisible by $\mathfrak{p}$.* (Weber, *Algebra*, Vol. II, p. 645.)

If in $\mathfrak{K}$ we decompose $\mathfrak{p}$ into factors, and write $\mathfrak{p}=\mathfrak{P}\mathfrak{a}$, and if we take the partial norm with respect to $\mathfrak{k}$, we have

$$\mathfrak{p}^n=\mathfrak{N}_\mathfrak{k}(\mathfrak{P})\cdot\mathfrak{N}_\mathfrak{k}(\mathfrak{a}). \tag{8}$$

From this it is seen that

$$\mathfrak{N}_t(\mathfrak{P}) = \mathfrak{p}^f,$$

where f is the *relative degree* of $\mathfrak{P}$ with respect to $\mathfrak{k}$.

If further f' is the degree of the prime ideal $\mathfrak{p}$ in $\mathfrak{k}$ with respect to the absolute realm R, so that

$$N_t(\mathfrak{p}) = p^{f'}, \tag{9}$$

it follows from (5) and (9) that

$$N_t(\mathfrak{P}) = p^{ff'}. \tag{10}$$

ART. 229. **Primitive Roots of the Prime Ideals.** We may write as above

$$N_t(\mathfrak{p}) = P \tag{1}$$

where $P = p^{f'}$ and

$$N_t(\mathfrak{P}) = P^f, \tag{2}$$

where f is the relative grade of $\mathfrak{P}$ with respect to $\mathfrak{k}$.

If ω is any integer in $\mathfrak{k}$, it was seen in Art. 38 that

$$\omega^P \equiv \omega \pmod{\mathfrak{p}};$$

and therefore also

$$\omega^P \equiv \omega \pmod{\mathfrak{P}}. \tag{3}$$

For every integer Ω of $\mathfrak{O}$ we have

$$\Omega^{P^f} \equiv \Omega \pmod{\mathfrak{P}}. \tag{4}$$

The number of incongruent, modulo $\mathfrak{p}$, integers in $\mathfrak{k}$ is P (Art. 38), while the number of incongruent, modulo $\mathfrak{P}$, integers in $\mathfrak{K}$ is P^f.

As in Art. 45, end, it may be proved that corresponding to every prime ideal $\mathfrak{P}$ there exist primitive roots Γ, that is, integers in $\mathfrak{K}$ which satisfy the congruence

$$\Gamma^{P^f-1} \equiv 1 \pmod{\mathfrak{P}}, \tag{5}$$

and which are such that no lower power of Γ with positive exponents is congruent to unity. It follows

that every integer Ω in $\mathfrak{K}$ which is not divisible by $\mathfrak{P}$ is congruent to one of the powers of Γ,

$$1, \Gamma, \Gamma^2, \cdots, \Gamma^{Pf-2} \tag{6}$$

with respect to the modulus $\mathfrak{P}$.

Next observe that every integer Ω satisfies in $\mathfrak{K}$ an irreducible equation of degree at most equal to n, whose coefficients are integers in $\mathfrak{k}$. This equation may also be regarded as a congruence, modulo $\mathfrak{P}$; and among such congruences there is one of the least degree, say

$$F(\Omega) \equiv 0 \pmod{\mathfrak{P}}.$$

In this congruence we may take the term of the highest power of Ω equal to unity. For if the coefficient (which is not divisible by $\mathfrak{P}$) is η_0 we may always find an integer η in $\mathfrak{k}$ such that

$$\eta_0\eta \equiv 1 \pmod{\mathfrak{P}}.$$

And we have only to multiply F by η to have the required result.

Hence if t is a variable, we may assume that the function F has the form

$$F(t) = t^\nu + \alpha_1 t^{\nu-1} + \alpha_2 t^{\nu-2} + \cdots + \alpha_\nu,$$

where the coefficients $\alpha_1, \cdots, \alpha_\nu$ are integers in $\mathfrak{k}$. Hence through division we may put any integral function $F_1(t)$ in the form

$$F_1(t) = Q(t)F(t) + \Phi(t), \tag{7}$$

where

$$\Phi(t) = \rho_0 + \rho_1 t + \cdots + \rho_{\nu-1} t^{\nu-1}, \tag{8}$$

the ρ's being integers in $\mathfrak{k}$, and where $Q(t)$ is an integral function in t, whose coefficients are integers in $\mathfrak{k}$ (including 0).

As we may take equation (5) as the one which $\Theta(=\Gamma)$ satisfies and for $F(t)$ in (7) any power of t, it follows from (6) that every integer Ω that is not divisible by $\mathfrak{P}$ satisfies

a congruence

$$\Omega \equiv \rho_0 + \rho_1 \Gamma + \cdots + \rho_{\nu-1}\Gamma^{\nu-1} \pmod{\mathfrak{P}}; \tag{9}$$

and since the ρ's may be zero, this is also true of an integer Ω that is divisible by $\mathfrak{P}$. (Art. 62.)

Observe that it is possible for each ρ in (9) to have P incongruent, modulo $\mathfrak{p}$, values; and that the number of incongruent, modulo $\mathfrak{P}$, values which Ω may have as expressed through (9) is P^ν. Since, as derived above, P^f is also this number, it is seen that $\nu = f$. It has been proved (Art. 42) that if $F(\Gamma) \equiv 0 \pmod{\mathfrak{P}}$, then also

$$F(\Gamma)^P \equiv F(\Gamma^P) \equiv 0 \pmod{\mathfrak{P}};$$

and similarly

$$F(\Gamma^{P^2}) \equiv 0, \quad \cdots, \quad F(\Gamma^{P^{f-1}}) \equiv 0 \pmod{\mathfrak{P}}.$$

With this is proved:

THEOREM I. *A primitive root Γ of $\mathfrak{P}$ satisfies with respect to $\mathfrak{P}$ a congruence in $\mathfrak{k}$ of the fth degree and the roots of this congruence are*

$$\Gamma, \ \Gamma^P, \ \Gamma^{P^2}, \ \cdots, \ \Gamma^{P^{f-1}}.$$

And this gives expression to the theorem:

THEOREM II. *The product*

$$(t-\Gamma)(t-\Gamma^2)\cdots(t-\Gamma^{P^{f-1}}) \tag{10}$$

is (mod. $\mathfrak{P}$) congruent to an integral function $F(t)$ in $\mathfrak{k}$.

ART. **230. Relative Discriminants.** Observe (Art. 227) that a basis of $\mathfrak{R}$ consists of mn numbers. Let β be a basis-form of $\mathfrak{O}$ and that is a linear form in mn indeterminates through which all the integers of $\mathfrak{O}$ may be expressed by writing for the indeterminates rational integers. We have then, say

$$F(t) = N_s(t-\beta), \tag{1}$$

which is an irreducible integral function of t with integral coefficients. Observe that $t = \beta$ is a root of this function.

Similarly let σ be a basis form of the integers in $\mathfrak{k}$, where σ is a linear form in m indeterminates, which in turn is the root of an irreducible function of the mth degree,

$$\psi(s) = N_{\mathfrak{k}}(s-\sigma), \tag{2}$$

whose coefficients are rational integers. (See Art. 193.)

From the function $F(t)$ may be factored out an irreducible function of the nth degree

$$f(t) = \mathfrak{N}_{\mathfrak{k}}(t-\beta), \tag{3}$$

whose coefficients are integers in $\mathfrak{k}$.

We may next prove the important theorem:

THEOREM. *The algebraic number $F'(\beta)$ is an associate of the product of the two numbers $f'(\beta)$ and $\psi'(\sigma)$.*

And that is

$$F'(\beta) = \epsilon f'(\beta)\psi'(\sigma), \tag{4}$$

where ϵ is a unit in $\mathfrak{R}$.

If next we form powers of the basis-form

$$\beta^h = U_{1h}\Omega_1 + U_{2h}\Omega_2 + \cdots + U_{mn,h}\Omega_{mn}$$

and observe [1] that the determinant of these linear forms is a unit, it is seen that every integer Ω in $\mathfrak{O}$ may be expressed in the form

$$\Omega = A_0 + A_1\beta + A_2\beta^2 + \cdots + A_{mn-1}\beta^{mn-1},$$

where the A's are integral functions.

If this expression is divided by $f(\beta)$, it follows (since $f(\beta) = 0$) that

$$\Omega = \alpha_0 + \alpha_1\beta + \cdots + \alpha_{n-1}\beta^{n-1}, \tag{5}$$

where the α's are integral in $\mathfrak{k}$. In the theory of Partial Fractions,[2] if $r_1, r_2, \cdots, r_l$ are the roots of a polynomial of

[1] Dedekind, "Ueber die Discriminanten endlicher Körper," *Gött. Abhandlungen*, 1882, Vol. 29; Weber, *Algebra*, Vol. II, pp. 648 ff.

[2] Burnside and Panton, *Theory of Equations*, 4th Edition, p. 172.

the lth degree, say $g(x)=0$, then is

$$\frac{r^m}{g'(r_1)}+\frac{r_2^m}{g'(r_2)}+\cdots+\frac{r_l^m}{g'(r_l)}=0,$$

if

$$m=1, 2, \cdots, l-2;$$

while this same summation is equal to 1, if $m=l-1$. It follows that

$$\mathfrak{S}_t\frac{\Omega}{f'(\beta)}=\alpha_{n-1}, \tag{6}$$

where α_{n-1} is an integer in $\mathfrak{k}$.

If this expression is multiplied by $1:\psi'(\sigma)$, it is seen, when α_{n-1} is expressed in terms of $1, \sigma, \sigma^2, \cdots, \sigma^{m-1}$, that

$$S_t\mathfrak{S}_t\frac{\Omega}{f'(\beta)\psi'(\sigma)}=S_*\frac{\Omega}{f'(\beta)\psi'(\sigma)}=S_t\frac{\alpha_{n-1}}{\psi'(\sigma)}=a, \tag{7}$$

where a is a rational integer.

Similarly expressing Ω in integral powers of β, it follows directly that

$$S_*\frac{\Omega}{F'(\beta)}=b, \tag{8}$$

where b is a rational integer. Next write

$$\Omega=\frac{F(t)}{t-\beta}=F_1(t), \tag{9}$$

where $F_1(t)$ is an integral function of the $mn-1$ degree in t, and express the coefficients of $F_1(t)$ through powers of β. It is seen that

$$S_*\frac{F_1(t)}{f'(\beta)\psi'(\sigma)}=\sum_{\nu=0}^{\nu=mn-1}a_\nu t^\nu, \tag{10}$$

where the a's are rational integers.

Write in this expression $t=\beta$, and it follows that

$$\frac{F'(\beta)}{f'(\beta)\psi'(\sigma)}=\sum_{\nu=0}^{\nu=mn-1}a_\nu\beta^\nu; \tag{11}$$

and from this it is seen that $F'(\beta)$ is divisible by $f'(\beta)\psi'(\sigma)$.

On the other hand again let s and t be two variables and write

$$\Omega=\frac{f(t)}{t-\beta}\cdot\frac{\psi(s)}{s-\sigma}=f_1(t)\psi_1(s). \tag{12}$$

It is seen that

$$S_{\mathfrak{R}}\frac{f_1(t)\psi_1(s)}{F'(\beta)}=\sum_{h=0}^{h=m-1}\sum_{k=0}^{k=n-1}b_{h,k}s^ht^k, \tag{13}$$

where $b_{h,k}$ are rational integers. Writing β and σ for t and s in this expression, we have

$$\frac{f_1(\beta)\psi_1(\sigma)}{F'(\beta)}=\sum^{h}\sum^{k}b_{h,k}\beta^k\sigma^h; \tag{14}$$

and from this it is seen that $f'(\beta)\psi'(\sigma)$ is divisible by $F'(\beta)$. Accordingly Theorem I is proved.

The two quantities $F'(\beta)$ and $\psi'(\sigma)$ (see Art. 106) are the *fundamental* ideals of the realms $\mathfrak{R}$ and $\mathfrak{k}$ and may be denoted by $G_{\mathfrak{R}}$ and $G_{\mathfrak{k}}$. It is also seen that

$$f'(\beta)=(\beta-\beta_1)(\beta-\beta_2)\cdots(\beta-\beta_{n-1}) \tag{15}$$

is an ideal, which may be denoted by $\mathfrak{G}_{\mathfrak{k}}$ and is the *relative fundamental* ideal of $\mathfrak{R}$ with respect to $\mathfrak{k}$. From (4) it is seen that

$$G_{\mathfrak{R}}=G_{\mathfrak{k}}\mathfrak{G}_{\mathfrak{k}}. \tag{16}$$

The *partial discriminant* $\mathfrak{D}_{\mathfrak{k}}$ of the realm $\mathfrak{R}$ may be defined as the partial norm of the relative fundamental ideal $\mathfrak{G}_{\mathfrak{k}}$; that is

$$\mathfrak{D}_{\mathfrak{k}}=\mathfrak{N}_{\mathfrak{k}}(\mathfrak{G}_{\mathfrak{k}}). \tag{17}$$

Observe that $\mathfrak{D}_{\mathfrak{k}}$ is an ideal in $\mathfrak{k}$.

If in (16) the partial norm is taken with respect to $\mathfrak{k}$, we have

$$\mathfrak{N}_{\mathfrak{k}}(\mathfrak{G}_{\mathfrak{R}})=G_{\mathfrak{k}}^n\mathfrak{D}_{\mathfrak{k}}. \tag{18}$$

If by $D_{\mathfrak{R}}$ and $D_{\mathfrak{k}}$ we denote the discriminants (fundamental invariants) of $\mathfrak{R}$ and $\mathfrak{k}$ we have

$$D_{\mathfrak{R}}=D_{\mathfrak{k}}^nN_{\mathfrak{k}}(\mathfrak{D}_{\mathfrak{k}}). \tag{19}$$

We thus have (see Art. 186):

THEOREM II. *The fundamental invariant of a realm is divisible by the fundamental invariant of every divisor of the realm, and in the fundamental invariant of the divisor there can appear no prime integers that do not divide the fundamental invariant of the realm.*

It may happen as in the case of the complex multiplication of the elliptic functions that the ideal $f'(\beta)$ is a unit. In this case the partial fundamental ideal $\mathfrak{G}_r$ may be replaced by a unit and from (17) it is seen that $N_r(\mathfrak{D}_r) = \pm 1$. In this case the fundamental invariant of $\mathfrak{R}$ is a power of the fundamental invariant of $\mathfrak{r}$, if the sign is neglected.

There is another theorem which is in a sense the inverse of Theorem II:

If $\mathfrak{R}_1$ and $\mathfrak{R}_2$ are two algebraic realms, we may form a third realm

$$\mathfrak{R} = \mathfrak{R}_1 \mathfrak{R}_2, \tag{20}$$

in which the numbers of $\mathfrak{R}_1$ are adjoined to those of $\mathfrak{R}_2$. If D, D_1 and D_2 are the fundamental invariants of the three realms, there exists the theorem:

THEOREM III. *D is divisible by all and only those prime integers which are divisors of either, or of both D_1 or D_2.*

Proof. Since $\mathfrak{R}_1$ and $\mathfrak{R}_2$ are divisors of $\mathfrak{R}$, it is seen from Theorem II that every prime integer that is a divisor of D_1 or D_2 must also divide D. To prove the inverse, form the realm $\mathfrak{R}_0$ consisting of all the numbers in $\mathfrak{R}$, $\mathfrak{R}_1$ and $\mathfrak{R}_2$ together with their conjugates. Denote its fundamental invariant by D_0. Let τ and σ be the bases (fundamental forms) of all the integers in $\mathfrak{R}_1$ and $\mathfrak{R}_2$ and observe that, if u and v are two indeterminates,

$$\eta = u\tau + v\sigma \tag{21}$$

is an integral form in $\mathfrak{R}$.

If $\tau^{(i)}$, $\tau^{(j)}$, $\sigma^{(h)}$, $\sigma^{(k)}$ are conjugate values of τ and σ respectively, the discriminant $D(\eta)$ consists of the product of factors

$$u(\tau^{(i)}-\tau^{(j)})+v(\sigma^{(h)}-\sigma^{(k)}). \tag{22}$$

Now observe that the prime ideals that may divide these factors in $\mathfrak{R}_0$ are of three kinds

(1) the prime factors of $\tau^{(i)}-\tau^{(j)}$, when $\sigma^{(h)}=\sigma^{(k)}$,

(2) the prime factors of $\sigma^{(h)}-\sigma^{(k)}$, when $\tau^{(i)}=\tau^{(j)}$,

(3) the prime factors of $u(\tau^{(i)}-\tau^{(j)})+v(\sigma^{(h)}-\sigma^{(k)})$, when $\tau^{(i)}\neq\tau^{(j)}$ and $\sigma^{(h)}\neq\sigma^{(k)}$.

The first prime factors are divisors of D_1, the second of D_2, while the third are factors of both D_1 and D_2. Hence there may appear as factors in $D(\eta)$ no prime numbers that do not divide either D_1 or D_2. And this is what was to be proved.

If Ω is a number of $\mathfrak{R}$, and if

$$f(t)=\mathfrak{N}_r(t-\Omega), \tag{23}$$

is an integral function of the nth degree in t, then

$$\mathfrak{N}_r f'(\Omega) \tag{24}$$

is the partial discriminant of the number Ω with respect to the realm $\mathfrak{k}$. It is a number of $\mathfrak{k}$; and if Ω is an integer in $\mathfrak{R}$, this discriminant is an integer in $\mathfrak{k}$.

The integers Ω are had by writing definite rational integers for the indeterminates that appear in the fundamental form β, and these same integers change $f'(\beta)$ into $f'(\Omega)$. And from this follows the theorem:

THEOREM IV. *The partial discriminant of any integer Ω in $\mathfrak{R}$ with respect to $\mathfrak{k}$ is divisible by the partial discriminant (fundamental invariant) of $\mathfrak{R}$ with respect to $\mathfrak{k}$.*

This theorem may be proved directly by using Theorem 35 in Hilbert's *Bericht.*

ART. 231. **Prime Ideals in Relative Normal Realms.** If the realms [see (3) of Art. 228]

$$\mathfrak{K} = \mathfrak{R}(\alpha, \Theta),\ \mathfrak{K}_1 = \mathfrak{R}(\alpha, \Theta_1),\ \cdots,\ \mathfrak{K}_{n-1} = \mathfrak{R}(\alpha, \Theta_{n-1})$$

are identical with one another; that is, if they are all equal to $\mathfrak{K}$, then $\mathfrak{K} = \mathfrak{R}(\alpha, \Theta, \Theta_1, \cdots, \Theta_{n-1})$ is a *normal realm with respect to* $\mathfrak{k}$ (*relative normal*).

The substitutions (Θ, Θ), (Θ, Θ_1), (Θ, Θ_2), $\cdots$, (Θ, Θ_{n-1}) through which any number in $\mathfrak{K}$ is transformed into its conjugates form a group, the group of the realm $\mathfrak{K}$ with respect to $\mathfrak{k}$. This group may be denoted by Φ and its substitutions by $\varphi, \varphi_1, \varphi_2, \cdots, \varphi_{n-1}$, so that

$$\Phi = \varphi, \varphi_1, \cdots, \varphi_{n-1}.$$

When this group is commutative, that is, if $\varphi_i\varphi_j = \varphi_j\varphi_i$ (i, j denoting any of the numbers $0, 1, \cdots, n-1$), then $\mathfrak{K}$ is said to be *commutative with respect to* $\mathfrak{k}$ (relative abelian); and if Φ is cyclic, *relative cyclic*.

We shall assume that the realm $\mathfrak{K}$ is relative normal, and denote by

(1) $$\Omega/\varphi_i$$

the number which results from Ω through the substitution φ_i. It follows from the definition that both these numbers belong to $\mathfrak{K}$. It is evident that any ideal $\mathfrak{J}$ through the substitution φ_i becomes another definite ideal $\mathfrak{J}/\varphi_i$ in $\mathfrak{K}$; and if Ω is any integer that is divisible by $\mathfrak{J}$, then is Ω/φ_i divisible by $\mathfrak{J}/\varphi_i$.

If $\mathfrak{J}$ is any ideal in $\mathfrak{K}$, there are certain substitutions ψ in Φ which satisfy the condition

(2) $$\mathfrak{J}/\psi = \mathfrak{J}.$$

Among these is the identical substitution. The substitutions ψ form a group Ψ which is a divisor of Φ.

We call Ψ the *group which belongs to* or *permits* the ideal $\mathfrak{J}$ and we say also that $\mathfrak{J}$ *belongs to* the group Ψ.

Likewise there are substitutions of Φ which leave unaltered the quantities of $\mathfrak{k}$. Any relation or equation existing among the numbers and ideals in $\mathfrak{K}$, when operated upon by such substitutions of Φ, offers a similar relation or equation among the conjugate numbers and ideals. It follows that units, integral ideals, the property of one being divisible by another, do not lose such characteristics when any of the substitutions of Φ is made.

This gives rise to the theorem:

THEOREM I. *If $\mathfrak{P}$ is a prime ideal in $\mathfrak{K}$, then all ideals $\mathfrak{P}/\varphi_i$, that are conjugate to $\mathfrak{P}$ in $\mathfrak{K}$, remain prime ideals in $\mathfrak{K}$. If $\mathfrak{J}$ is divisible by any power of $\mathfrak{P}$ then $\mathfrak{J}/\varphi_i$ is divisible by the same power of $\mathfrak{P}/\varphi_i$.*

In Art. 228 it was seen that there is only one prime ideal $\mathfrak{p}$ in $\mathfrak{k}$ which is divisible by $\mathfrak{P}$. If f is the relative degree of $\mathfrak{P}$, we have

$$\mathfrak{N}_{\mathfrak{k}}(\mathfrak{P}) = \mathfrak{p}^f; \tag{3}$$

and since the norm of an ideal is equal to the product of all its conjugate ideals, it is seen that $\mathfrak{p}$ is divisible only by the ideals $\mathfrak{P}/\varphi_i$ that are conjugate with $\mathfrak{P}$ in $\mathfrak{k}$. Further since (with respect to $\mathfrak{k}$) the ideals $\mathfrak{P}/\varphi_i$ all have the same norm, they also have the same relative degree f.

If $\mathfrak{P}^g$ is the highest power of $\mathfrak{P}$ that divides $\mathfrak{p}$, it follows from Theorem I that $\mathfrak{p}$ is also divisible by the gth power of all the conjugate prime factors of $\mathfrak{P}$ and by no higher power of these ideals.

If then $\mathfrak{P}_1, \mathfrak{P}_2, \cdots, \mathfrak{P}_e$ are the different prime ideals that are conjugate with $\mathfrak{P}$, it is seen that

$$\mathfrak{p} = (\mathfrak{P}_1\mathfrak{P}_2 \cdots \mathfrak{P}_e)^g. \tag{4}$$

If the partial norm is taken of both sides of this expression, and if n is the degree of the realm $\mathfrak{K}$ with respect to $\mathfrak{k}$

so that the partial norm of $\mathfrak{p}$ is $\mathfrak{p}^n$, it follows from (3) that

$$n = efg. \tag{5}$$

From this it is seen that the integers e, f, g are divisors of n.

If $\mathfrak{P}$ is transformed into $\mathfrak{P}_1$ through the substitution φ_1, and that is, if $\mathfrak{P}_1 = \mathfrak{P}/\varphi_1$, then is

$$\mathfrak{P} = \mathfrak{P}_1/\varphi_1^{-1}. \tag{a}$$

Further if Ψ is the group that belongs to $\mathfrak{P}$, then for every substitution ψ in Ψ, we have

$$\mathfrak{P}_1 = \mathfrak{P}/\psi\varphi_1 \qquad \text{or from } (a) \qquad \mathfrak{P}_1 = \mathfrak{P}_1/\varphi_1^{-1}\psi\varphi_1.$$

Inversely, if $\mathfrak{P}_1/\varphi = \mathfrak{P}_1$, it follows that $\mathfrak{P}/\varphi_1\varphi\varphi_1^{-1} = \mathfrak{P}$, so that $\varphi_1\varphi\varphi_1^{-1} = \psi$ or $\varphi = \varphi_1^{-1}\psi\varphi_1$; and that is, $\mathfrak{P}_1$ belongs to the group $\varphi_1^{-1}\Psi\varphi_1$. Further if

$$\mathfrak{P}_1 = \mathfrak{P}/\varphi_1,\ \mathfrak{P}_2 = \mathfrak{P}/\varphi_2,\ \cdots,\ \mathfrak{P}_e = \mathfrak{P}/\varphi_e,$$

it is seen that

$$\Phi = \Psi\varphi_1 + \Psi\varphi_2 + \cdots + \Psi\varphi_e. \tag{6}$$

And that is, Ψ is a divisor of Φ of index e and of degree fg. If

$$\beta = t_1\Omega_1 + t_2\Omega_2 + \cdots + t_{mn}\Omega_{mn} \tag{7}$$

is a basis form of $\mathfrak{O}$, there exist certain substitutions χ in Φ, and always the identical substitution, which satisfy the congruence

$$\beta/\chi \equiv \beta \pmod{\mathfrak{P}}. \tag{8}$$

All these substitutions form a group X. This group is a divisor of Ψ, to which $\mathfrak{P}$ belongs. For observe that we may derive from β a basis form for $\mathfrak{P}$ as follows:

For the t's in (7) we have to write certain linear functions of new variables and rational integral coefficients, as in Vol. I, Art. 148. If then π is a basis form of $\mathfrak{P}$, it follows from (8) that π/χ is divisible by π and therefore also

$$\mathfrak{P}/\chi = \mathfrak{P}.$$

Next observe that β satisfies in $\mathfrak{k}$ an equation $f(t)=0$ of the nth degree.

Denote its roots by $\beta_1, \beta_2, \cdots, \beta_n$, which are in $\mathfrak{k}$ conjugate forms of β with coefficients integral in $t_1, t_2, \cdots$. Accordingly we may write (if t is a new variable)

$$(9) \quad f(t, t_1, t_2, \cdots) = f(t) = (t-\beta_1)(t-\beta_2)\cdots(t-\beta_n).$$

This expression raised to powers of p gives, modulo $\mathfrak{P}$,

$$(10) \quad f(t^P, t_1^P, t_2^P, \cdots) \equiv [f(t)]^P \equiv (t^P-\beta_1')(t^P-\beta_2')\cdots(t^P-\beta_n'),$$

where the β''s are derived from the β's by writing $t_1^P, t_2^P, \cdots$ in the place of $t_1, t_2, \cdots$, and $P = N_{\mathfrak{k}}(\mathfrak{p})$.

If we put $t=\beta$ in (10) it is seen that $f(t)$ becomes zero and that one of the factors of the product is divisible by $\mathfrak{P}$; and that is, there exists a substitution, say ψ_0 of Φ, which satisfies the condition

$$(11) \qquad \beta^P \equiv \beta'/\psi_0 \pmod{\mathfrak{P}}.$$

All the integers in $\mathfrak{K}$ are had, if for the indeterminates t_1, $t_2 \cdots$ in β we write rational integers. Due to the Fermat Theorem for rational integers, it is seen that the formulas (8) and (11) have the same meaning as the following formulas which are true of every integer Ω in $\mathfrak{K}$, namely,

$$(12) \qquad \Omega/\chi \equiv \Omega, \qquad \Omega^P \equiv \Omega/\psi_0 \pmod{\mathfrak{P}}.$$

From the second of these congruences it is seen that if the integer Ω is divisible by $\mathfrak{P}$ then also Ω/ψ_0 is divisible by $\mathfrak{P}$ and *vice versa*. It follows that $\mathfrak{P} = \mathfrak{P}/\psi_0$ and therefore that ψ_0 is one of the substitutions of Ψ.

It was seen at the end of Art. 229 that

$$(13) \quad (t-\gamma)(t-\gamma^P)\cdots(t-\gamma^{P^{f-1}}) \equiv F(t) \pmod{\mathfrak{P}},$$

where γ is a primitive root of $\mathfrak{P}$ and $F(t)$ is an integral function of t in $\mathfrak{k}$. It follows that

$$F(\gamma) \equiv 0 \pmod{\mathfrak{P}};$$

and if ψ is any substitution of Ψ, that

$$F(\gamma/\psi) \equiv 0 \pmod{\mathfrak{P}/\psi} \quad \text{or} \quad F(\gamma/\psi) \equiv 0 \pmod{\mathfrak{P}}.$$

From this it results that γ/ψ must be congruent, modulo $\mathfrak{P}$, to one of the powers of γ that appears in (13), say

$$\gamma^{P^\nu} \equiv \gamma/\psi \pmod{\mathfrak{P}}. \tag{14}$$

We have seen that every integer of $\mathfrak{O}$, which is not divisible by $\mathfrak{P}$, is congruent (mod. $\mathfrak{P}$) to one of the powers of γ that appears in (13).

If $\Omega \equiv \gamma^{P^\mu} \pmod{\mathfrak{P}}$, it follows from (14) that

$$(\gamma^{P^\mu})^{P^\nu} \equiv (\gamma/\psi)^{P^\mu} \pmod{\mathfrak{P}},$$

or

$$\Omega^{P^\nu} \equiv \Omega/\psi \pmod{\mathfrak{P}}. \tag{15}$$

This congruence is also true, if Ω is divisible by $\mathfrak{P}$, and hence in general it is true for all integers of $\mathfrak{K}$. If application is made ν times of the second formula in (12), we have

$$\Omega^{P^\nu} \equiv \Omega/\psi_0^\nu \pmod{\mathfrak{P}}. \tag{16}$$

We therefore have

$$\Omega/\psi \equiv \Omega/\psi_0^\nu \pmod{\mathfrak{P}}. \tag{17}$$

If for Ω we put Ω/ψ^{-1} and apply the substitution ψ^{-1} to (17), we have

$$\Omega \equiv \Omega/\psi^{-1}\psi_0^\nu \equiv \Omega/\psi_0^\nu\psi^{-1} \pmod{\mathfrak{P}}. \tag{18}$$

It follows that both the substitutions $\psi^{-1}\psi_0^\nu$ and $\psi_0^\nu\psi^{-1}$ are among those of the group X; and it is thus seen that every substitution ψ of Ψ is found in one of the sub-groups

$$\mathrm{X},\ \mathrm{X}\psi_0,\ \mathrm{X}\psi_0^2,\ \cdots.$$

If in (16) we write $\nu = f$, that congruence becomes

$$\Omega \equiv \Omega/\psi_0^f,$$

so that ψ_0 to the fth power, and to no lower power, is a substitution of X. With this it is seen that the sub-groups

$$\mathrm{X},\ \mathrm{X}\psi_0,\ \mathrm{X}\psi_0^2,\ \cdots,\ \mathrm{X}\psi_0^{f-1}$$

are all different and are all substitutions of Ψ, with the

result that

$$\Psi = X + X\psi_0 + \cdots + X\psi_0'^{-1}. \tag{19}$$

It may be proved next that the complex of substitutions $\psi_0^\nu X$ is identical with the complex $X\psi_0^\nu$ for every ν. For from (16) and (12) it is seen that

$$\Omega^{P^\nu}/\psi_0^{-\nu} \equiv \Omega \qquad \text{and} \qquad \Omega^{P^\nu}/\psi_0^{-\nu}\chi\psi_0^\nu \equiv \Omega^{P^\nu} \pmod{\mathfrak{P}}.$$

It follows that $\psi_0^{-\nu}\chi\psi_0^\nu$ is a substitution in X. Accordingly we have

$$\psi_0^\nu X = X\psi_0^\nu, \tag{20}$$

and that is, X is a normal divisor of Ψ. We saw above *that Ψ is of degree gf, so that from (19) X is of degree g.*

Hence the group Ψ/X is cyclic and of degree f.

ART. 232. **Ideals in the Divisors of the Realm $\mathfrak{R}$.** If the group Φ of the realm $\mathfrak{R}$ has a divisor Φ', then to Φ' there belongs a realm $\mathfrak{R}'$, which is a divisor of $\mathfrak{R}$ and which has $\mathfrak{k}$ as a divisor.

The numbers of $\mathfrak{R}'$ through the substitutions Φ' remain unchanged. And Φ' is the group of the realm $\mathfrak{R}$ with respect to $\mathfrak{R}'$; and that is, if a quantity ψ that permits Φ' is added to the stock-realm $\mathfrak{k}$, then the group Φ in the extended stock-realm reduces to the group Φ'. (Art. 221, Theorem III.)

We may denote by n' the degree of the group Φ', which being a divisor of the degree of Φ may be written

$$n = n'm'. \tag{1}$$

From this it is seen that n' is the degree of $\mathfrak{R}$ with respect to $\mathfrak{R}'$ and m' is the degree of $\mathfrak{R}'$ with respect to $\mathfrak{k}$.

It may be observed that $\mathfrak{R}$ is a normal realm with respect to $\mathfrak{R}'$ but in general $\mathfrak{R}'$ is not a normal realm with respect to $\mathfrak{k}$.

The prime ideals in $\mathfrak{R}'$ may be derived from those of $\mathfrak{R}$ as follows:

If $\mathfrak{P}$ is a prime ideal in $\mathfrak{R}$, there is one and only one prime ideal in $\mathfrak{R}'$, say $\mathfrak{P}'$, which is divisible by $\mathfrak{P}$. Further $\mathfrak{p}$ in $\mathfrak{k}$ is divisible by $\mathfrak{P}$ and its conjugates in $\mathfrak{R}$. It follows that $\mathfrak{P}'$ is divisible by $\mathfrak{P}$ and its conjugates in $\mathfrak{R}'$. If φ' runs through the substitutions of Φ', then $\mathfrak{P}'$ remains unaltered. It follows that $\mathfrak{P}'$ is also divisible by $\mathfrak{P}/\varphi'$.

Observe next that if $\mathfrak{P}'_1$, is divisible by $\mathfrak{P}/\varphi_1$ then it is also divisible by $\mathfrak{P}/\psi\varphi_1\varphi'$, where ψ is an arbitrary substitution of the group Ψ of the preceding article.

If then φ is an element of the system

$$\Phi_1 = \Psi\varphi_1\Phi',$$

then is $\mathfrak{P}'_1$ divisible by $\mathfrak{P}/\varphi$.

If φ_2 is an element of Φ which does not appear in Φ_1, the system

$$\Phi_2 = \Psi\varphi_2\Phi'$$

has no elements in common with Φ_1 (see Art. 224). If there is an element φ_3 which appears in neither Φ_1 nor Φ_2 we form

$$\Phi_3 = \Psi\varphi_3\Phi'$$

and continue until all the elements of Φ have been accounted for. We thus have

$$\Phi = \Phi_1 + \Phi_2 + \cdots + \Phi_\sigma. \tag{2}$$

And from Art. 224 it is seen that the degree of any one of these systems, Φ_r say, is found to be the product of the degrees of Ψ and Φ' divided by the degree, h_r say, of the intersection of Φ' and $\Psi_r = \varphi_r^{-1}\Psi\varphi_r$. Accordingly the degree of Φ_r equals $fgn' : h_r$.

If φ_r goes over all the elements of Φ_r, the prime ideals $\mathfrak{P}/\varphi_r$ are all transformed into the same prime ideal $\mathfrak{P}'_r$ in $\mathfrak{R}'$.

It must be proved that any two different systems, say Φ_1 and Φ_2 lead to different ideals $\mathfrak{P}'_1$ and $\mathfrak{P}'_2$. Note that if

$\mathfrak{P}/\varphi_1 = \mathfrak{P}/\varphi_2$, then is $\mathfrak{P} = \mathfrak{P}/\varphi_2\varphi_1^{-1}$, and that is, $\varphi_2\varphi_1^{-1}$ is an element of Ψ, or φ_2 is found in $\Psi\varphi_1$, and that is in Φ_1 which is contrary to the hypothesis.

We may accordingly determine an integer A in $\mathfrak{K}$, which is divisible by the ideal $\mathfrak{P}/\varphi_1$ (where φ_1 goes through the elements of Φ_1), but by none of the ideals $\mathfrak{P}/\varphi_2$ when φ_2 goes through the elements of Φ_2. It is seen that none of the integers A/φ' is divisible by $\mathfrak{P}/\varphi_2$; otherwise we should have $\mathfrak{P}/\varphi_1\varphi' = \mathfrak{P}/\varphi_2$ contrary to the assumption that φ_2 was not contained in Φ_1.

Hence the product A' of all the different integers A/φ', as φ' goes through all the elements of Φ', is an integer in $\mathfrak{K}'$ which is divisible by $\mathfrak{P}_1'$ but not by $\mathfrak{P}_2'$. It follows that $\mathfrak{P}_1'$ is different from $\mathfrak{P}_2'$ and that accordingly there are e' and no more different prime ideals $\mathfrak{P}'$ in $\mathfrak{p}$.

We may therefore put

$$\mathfrak{p} = \mathfrak{P}_1'^{a_1}\mathfrak{P}_2'^{a_2}\cdots\mathfrak{P}_{e'}'^{a_{e'}}, \tag{3}$$

where the rational integers $a_1, a_2, \cdots, a_{e'}$ are yet to be determined.

To factor the prime ideals $\mathfrak{P}_r'$ in the realm $\mathfrak{K}$, we may simply let $\mathfrak{K}'$ take the place of $\mathfrak{k}$ in the preceding article and use the results there given. Define X_r by the relation

$$\mathrm{X}_r = \varphi_r^{-1}\mathrm{X}\varphi_r$$

and let X_r' denote the intersection of Φ' with X_r; that is, X_r' denotes the complex of substitutions of Φ', which satisfy the condition

$$\beta/\chi_r' \equiv \beta \pmod{\mathfrak{P}_r}.$$

If there are g_r substitutions in the group X_r', then [see (4) of the preceding article] $\mathfrak{P}_r'$ is divisible by $\mathfrak{P}_r'^{g_r}$ but no higher power of $\mathfrak{P}_r$. Observe (at end of the last article) that g is the degree of X and gf that of Ψ.

The intersection Ψ'_r of Ψ_r and Φ', whose degree was denoted above by h_r, is the complex of all substitutions Ψ'_r in Φ' which satisfy the condition

$$\mathfrak{P}_r/\psi'_r=\mathfrak{P}_r.$$

If then Φ' is decomposed into sub-groups

$$\Phi'=\Psi'_r\varphi'_{r,1}+\Psi'_r\varphi'_{r,2}+\cdots+\Psi'_r\varphi'_{r,e_r}, \tag{4}$$

we have

$$n'=e_rh_r. \tag{5}$$

If we put

$$\mathfrak{P}_{r,s}=\mathfrak{P}/\varphi_{r,s},$$

it follows, see (4) and (6) of the preceding article, that

$$\mathfrak{P}'_r=(\mathfrak{P}_{r,1}\mathfrak{P}_{r,2}\cdots\mathfrak{P}_{r,e_r})^{g_r}. \tag{6}$$

Through the substitutions of (6) in (3) it follows from (4) of the preceding article that

$$g=a_rg_r, \qquad e=e_1+e_2+\cdots+e_{s'}, \tag{7}$$

through which the exponents a_r are defined.

The partial norm of $\mathfrak{P}_{r,s}$ with respect to $\mathfrak{K}'$ is [see (3) and (5) of the preceding article]

$$\mathfrak{N}_{\mathfrak{K}'}(\mathfrak{P}_{r,s})=\mathfrak{P}'^{f_r}_r, \tag{8}$$

where f_r is defined through the equation

$$n'=e_rf_rg_r=e_rh_r \text{ [see (5)]}. \tag{9}$$

We shall next decompose the group Φ into sub-groups with respect to Φ'; and write, if $\sigma_1, \sigma_2, \cdots, \sigma_{m'}$ are suitably chosen substitutions of Φ,

$$\Phi=\Phi'\sigma_1+\Phi'\sigma_2+\cdots+\Phi'\sigma_{m'}, \tag{10}$$

so that through the substitutions $\sigma_1, \sigma_2, \cdots, \sigma_{m'}$, the realm $\mathfrak{K}'$ is transformed into the conjugate (equal or different) realms

$$\mathfrak{K}'_1, \mathfrak{K}'_2, \cdots, \mathfrak{K}'_{m'}.$$

The realm $\mathfrak{K}'_i$ accordingly belongs to the group $\sigma_i^{-1}\Phi'\sigma_i$. If then through σ_i the ideals $\mathfrak{P}'_r$ and $\mathfrak{P}_{r,s}$ are transformed

into $\mathfrak{P}'_{r,t}$ and $\mathfrak{P}_{r,s,t}$, it follows from (4) of the preceding article that

$$\mathfrak{P}'_{r,t} = (\mathfrak{P}_{r,1,t}\mathfrak{P}_{r,2,t}\cdots\mathfrak{P}_{r,e_r,t})^{g_r}, \tag{11}$$

and the product of these ideals for $t=1, 2, \cdots, m'$ is the partial norm taken in $\mathfrak{K}'$ of $\mathfrak{P}'_r$ with respect to the realm $\mathfrak{k}$, and which we denote by $\mathfrak{N}'_t(\mathfrak{P}'_r)$.

This norm must be a power of $\mathfrak{p}$, say

$$\mathfrak{N}'_t(\mathfrak{P}'_r) = \mathfrak{p}^{f'_r}. \tag{12}$$

To determine f'_r we must decompose $\mathfrak{p}$ in (12) into its prime factors $\mathfrak{P}$ as indicated in (4) of the preceding article, from which there are found to be egf'_r prime factors $\mathfrak{P}$ in $\mathfrak{p}^{f'_r}$. On the other hand there are seen to be $g_r e_r m'$ such factors in the product of the m' factors (11).

It follows that

$$egf'_r = m'g_re_r = \frac{n}{n'}g_re_r = \frac{efg}{e_rf_rg_r}g_re_r \tag{13}$$

or

$$f = f_r f'_r. \tag{14}$$

In this formula f_r denotes the degree of the ideal $\mathfrak{P}_r$ with respect to $\mathfrak{K}'$, while f'_r denotes the degree of $\mathfrak{P}'_r$ with respect to $\mathfrak{k}$. Thus agreeing with the results of Art. 228, formula (14) gives the degree f of $\mathfrak{P}_r$ with respect to $\mathfrak{k}$.

ART. 233. **The Divisor Realms Which Belong to a Prime Ideal.** An important application may be made of the preceding theorems. It has to do with the theory of the divisor realms which may be derived from the prime ideals of a realm $\mathfrak{K}$.

As hitherto let $\mathfrak{K}$ be a realm which with respect to $\mathfrak{k}$ is a normal realm of relative degree n and let $\mathfrak{P}$ be a prime ideal in $\mathfrak{K}$ which divides a rational prime p in $\mathfrak{K}$ and which also divides $\mathfrak{p}$ in $\mathfrak{k}$. If $\mathfrak{k}=R$ is the absolute realm, then is $\mathfrak{p}=p$. If as above

$$\mathfrak{p} = (\mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_e)^g, \qquad \mathfrak{N}(\mathfrak{P}) = \mathfrak{p}^f, \tag{1}$$

we have, as in (5) Art. 231,

$$n = efg; \tag{2}$$

and in the realm $\mathfrak{R}$ the group Ψ is of degree fg and the substitutions ψ of Ψ satisfy the relation

$$\mathfrak{P}/\psi = \mathfrak{P}. \tag{3}$$

To the group Ψ there belongs a realm in $\mathfrak{R}$, say $\mathfrak{R}_\psi$, which Hilbert called the *reduction* (*Zerlegungs*) or *separation* realm of $\mathfrak{P}$.

To apply the theorems of the preceding article to this realm and particularly to the prime ideal $\mathfrak{P}$, we have to write

$$\Phi' = \Psi, \quad \varphi_1 = 1, \quad \Phi_r = \Phi_1 = \Psi, \quad \Psi_r = \Psi_1 = \Psi; \tag{4}$$

$$n' = fg, \qquad m' = e, \qquad h_r = h_1 = fg. \tag{5}$$

It follows from the preceding article [see (7)] that

$$\mathrm{X}_r = \mathrm{X}, \qquad g_r = g, \qquad a_r = a_1 = 1.$$

If $\mathfrak{p}'$ is the prime ideal in $\mathfrak{R}_\psi$ that is divisible by $\mathfrak{p}$, we may write

$$\mathfrak{p}' = \mathfrak{p}\mathfrak{A}, \tag{6}$$

where $\mathfrak{A}$ is not divisible by $\mathfrak{P}$.

It follows from (5) above and from (9) of the preceding article that

$$e_r = e_1 = 1, \tag{7}$$

and consequently, see (11) of the same article,

$$\mathfrak{p}' = \mathfrak{P}^g. \tag{8}$$

From the formulas (6) and (8) it is seen that through the introduction of the realm $\mathfrak{R}_\psi$ the ideal $\mathfrak{P}$ in $\mathfrak{R}$ is separated from all the other prime ideals that are divisors of $\mathfrak{p}$. Hence the name *reduction* (or *separation*) realm.

From (13) and (14) of the preceding article it is also seen that

$$f'_r = f'_1 = 1; \qquad f_r = f_1 = f; \tag{9}$$

and accordingly we have the theorem:

THEOREM I. *In the separation realm* $\mathfrak{R}_\psi$, $\mathfrak{P}^\sigma$ *is a prime ideal of the first degree with respect to* $\mathfrak{k}$; *and* $\mathfrak{P}$ *is with respect to* $\mathfrak{R}_\psi$ *of degree* f, *being of the same degree with respect to* $\mathfrak{k}$. *And further*

$$\mathfrak{p}' = \mathfrak{P}^\sigma, \qquad \mathfrak{p} = \mathfrak{p}'\mathfrak{A},$$

where $\mathfrak{A}$ *is relatively prime to* $\mathfrak{P}$.

As a second application of the results of the preceding article, we may take the group X instead of Φ' of Art. 232, where the substitutions of X are defined through

$$\beta/\chi \equiv \beta \pmod{\mathfrak{P}}. \tag{10}$$

The realm which belongs to this group and which has as divisor $\mathfrak{R}_\psi$ is denoted by $\mathfrak{R}_X$. Instead of the realm $\mathfrak{k}$ we may take the realm $\mathfrak{R}_\psi$ as the realm of rationality and we may let the realms $\mathfrak{R}_X$ and $\mathfrak{R}_\psi$ take the place of the realms $\mathfrak{R}$ and $\mathfrak{R}'$ in the theory of the preceding articles. Noting that here $\varphi = 1$, observe that to

$$\begin{array}{ll} & \Phi,\ \Phi',\ \Psi,\ \mathrm{X},\ \Phi_r,\ \Psi_r,\ \mathrm{X}_r,\ \mathfrak{p}, \\ \text{correspond} & \Psi,\ \mathrm{X},\ \Psi,\ \mathrm{X},\ \Psi,\ \Psi,\ \mathrm{X},\ \mathfrak{p}'. \end{array}$$

Further observe that here the degree of Ψ is $n'm' = fg$, the degree of X being g. It was seen that Φ_r is of degree $fgn' : h_r$ and here $\Phi_r = \Psi$ is of degree fg. It follows that $n' = h_r$. Due to (8) above and (4) of Art. 231 and (11) of Art. 232, it is seen that

$$e = 1, \quad n' = g, \quad m' = f, \quad h_r = h_1 = g, \quad g_r = g,$$
$$a_r = a_1 = 1, \quad e_r = e_1 = 1, \quad e' = 1.$$

Accordingly, if we denote by $\mathfrak{p}''$ the prime ideal of the realm $\mathfrak{R}_X$ which is divisible by $\mathfrak{P}$, we have

$$\mathfrak{p}'' = \mathfrak{p}' = \mathfrak{P}^\sigma. \tag{11}$$

From this it is seen that the prime ideal $\mathfrak{p}'$ of the reduction realm is no further factored in the realm $\mathfrak{R}_X$ and due to this property the realm $\mathfrak{R}_X$ was called by Hilbert the *inertia realm*.

From Art. 232, (13) and (14), it is seen that

$$f'_r = f'_1 = f; \qquad f_r = f_1 = 1.$$

Accordingly we have the theorem:

THEOREM II. *In the inertia realm* $\mathfrak{K}_x$ *we have* $\mathfrak{p} = \mathfrak{p}''\mathfrak{A}$, *where* $\mathfrak{p}''$ *is a prime ideal of the inertia realm and* $\mathfrak{A}$ *is not divisible by* $\mathfrak{p}''$. *The prime ideal* $\mathfrak{p}' = \mathfrak{P}^g$ *of the reduction realm is no further factorable in the inertia realm. Its degree is* f *with respect to the reduction realm, while* $\mathfrak{P}$ *with regard to the inertia realm is of the first degree.*

Further, due to the theorem regarding the relative degree of prime ideals (Art. 229), there may be added:

THEOREM III. *The ideal* $\mathfrak{p}'' = \mathfrak{P}^g$ *in* $\mathfrak{K}$ *is of the* f*th degree with respect to* $\mathfrak{k}$.

From this an important property of the inertia realm may be deduced. We saw (Art. 229) that the number of incongruent integers, modulo $\mathfrak{P}$, of $\mathfrak{K}$ is

$$N_{\mathfrak{k}}(\mathfrak{P}) = P^f.$$

From Theorem III it is seen that the number of incongruent integers, modulo $\mathfrak{p}'$, of the inertia realm is equally large. From this follows the theorem:

THEOREM IV. *Every integer of the realm* $\mathfrak{K}$ *is congruent (mod.* $\mathfrak{P}$*) to an integer of the inertia realm* X.

From (19) of Art. 231, we have further

THEOREM V. *The inertia realm is relatively cyclic of degree* f *with respect to the separation realm, and its group is* Ψ/X.

The group Ψ is also called the *reduction group* and X the *inertia group* of the ideal $\mathfrak{P}$.

ART. 234. **The Branch-Group.** In the inertia group X there exist in general other groups, which are of significance for the prime ideal $\mathfrak{P}$ and which Hilbert [1] has investigated. One of these is the branch-group.

[1] Hilbert, *Die Theorie der algebraischen Zahlkörper*, § 43. And Weber, *Algebra*, Vol. II, pp. 664 ff.

To define this group, take a primitive integer $\tilde{\omega}$ of $\mathfrak{R}$ which is divisible by $\mathfrak{P}$ but not by $\mathfrak{P}^2$ (see Art. 63).

If χ is a substitution of X, then is $\tilde{\omega}/\chi$ divisible by $\mathfrak{P}$, but not by $\mathfrak{P}^2$, and the congruence

$$\tilde{\omega}/\chi \equiv \tilde{\omega}\xi \pmod{\mathfrak{P}^2}$$

admits a solution ξ, modulo $\mathfrak{P}$, which is not divisible by $\mathfrak{P}$. If γ is a primitive root of $\mathfrak{P}$, we may determine for every χ of X an exponent λ such that

$$\tilde{\omega}/\chi \equiv \gamma^{\lambda}\tilde{\omega} \pmod{\mathfrak{P}^2}. \tag{1}$$

Besides the identical substitution, there may be other substitutions χ, of X, which satisfy the congruence

$$\tilde{\omega}/\chi_1 \equiv \tilde{\omega} \pmod{\mathfrak{P}^2}.$$

The substitutions χ_1 form a group. And this gives rise to the definition: *The group* X_1 *of all the substitutions of* X, *which satisfy the condition*

$$\tilde{\omega}/\chi_1 \equiv \tilde{\omega} \pmod{\mathfrak{P}^2} \tag{2}$$

is called the branch-group of the prime ideal $\mathfrak{P}$.

We shall next prove the theorem:

THEOREM. *The degree* g_1 *of the branch-group* X_1 *is a power of* p.

From the congruence (2) we may derive the equation

$$\tilde{\omega}/\chi_1 = \tilde{\omega} + \alpha\tilde{\omega}^2, \tag{3}$$

where α, which is not necessarily integral, is such that its numerator is not divisible by $\mathfrak{P}$. It follows that, if we raise (3) to the νth power and apply the Binomial Theorem, we have for every exponent ν

$$\tilde{\omega}^{\nu}/\chi_1 \equiv \tilde{\omega}^{\nu} \pmod{\mathfrak{P}^{\nu+1}}. \tag{4}$$

Note that any substitution χ of X applied to any integer β of $\mathfrak{R}$ offers the congruence

$$\beta/\chi \equiv \beta \pmod{\mathfrak{P}}. \tag{5}$$

Further determine an integer β through the congruence

$$\tilde{\omega}/\chi_1 \equiv \tilde{\omega}+\beta\tilde{\omega}^2 \pmod{\mathfrak{P}^3}.$$

It follows that

$$\omega/\chi_1^2 \equiv (\tilde{\omega}+\beta\tilde{\omega}^2)/\chi_1 \equiv \tilde{\omega}+\beta\tilde{\omega}^2+\beta(\tilde{\omega}+\beta\tilde{\omega}^2)^2$$
$$\equiv \tilde{\omega}+2\beta\tilde{\omega}^2 \pmod{\mathfrak{P}^3}.$$

By a repetition of this process it is seen that

$$\tilde{\omega}/\chi_1^r \equiv \tilde{\omega}+r\beta\tilde{\omega}^2 \pmod{\mathfrak{P}^3}.$$

If in this expression we put $p=r$, it follows that

$$\tilde{\omega}/\chi_1^p \equiv \tilde{\omega} \pmod{\mathfrak{P}^3}.$$

Continuing, it is seen that

$$\tilde{\omega}/\chi_1^{p+1} \equiv \tilde{\omega}/\chi_1 \equiv \tilde{\omega}+\beta\tilde{\omega}^2 \pmod{\mathfrak{P}^3},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\tilde{\omega}/\chi_1^{p^2} \equiv \tilde{\omega} \pmod{\mathfrak{P}^4};$$

and in general

$$\tilde{\omega}/\chi_1^{p^\nu} \equiv \tilde{\omega} \pmod{\mathfrak{P}^{\nu+2}}. \tag{7}$$

Since $\tilde{\omega}$ is a primitive integer in $\mathfrak{K}$, every substitution φ of Φ, excepting the identical substitution, causes the difference $\tilde{\omega}/\varphi-\tilde{\omega}$ to be different from zero. Accordingly there exists a sufficiently high power $\mathfrak{P}^\mu$ such that all these differences are not divisible by $\mathfrak{P}^\mu$; and if in (7) we choose the exponent $\nu+2 \geqq \mu$, it follows that

$$\chi_1^{p^\nu} = 1.$$

From this it is seen that the degree of every element χ_1 of X_1, and consequently the degree of X_1 itself is a power of p, as was to be proved.

If χ and χ' are any two elements of X, two exponent λ and λ' [due to (1)] may be so chosen that

$$\tilde{\omega}/\chi \equiv \gamma^\lambda\tilde{\omega}, \qquad \tilde{\omega}/\chi' \equiv \gamma^{\lambda'}\tilde{\omega} \pmod{\mathfrak{P}}; \tag{8}$$

and from this it is seen that, due to (5),

$$\tilde{\omega}/\chi\chi' \equiv \gamma^{\lambda+\lambda'}\tilde{\omega} \pmod{\mathfrak{P}^2}. \tag{9}$$

Consequently there exist simultaneously the congruences

$$\tilde{\omega}/\chi \equiv \gamma^{\lambda}\tilde{\omega}, \qquad \tilde{\omega}/\chi^{-1} \equiv \gamma^{-\lambda}\tilde{\omega} \pmod{\mathfrak{P}^2}.$$

If χ_1 is an element of X_1, it is seen that

$$\tilde{\omega}/\chi^{-1}\chi_1\chi \equiv \tilde{\omega} \pmod{\mathfrak{P}^2}, \tag{10}$$

and therefore $\chi^{-1}\chi_1\chi$ belongs to X_1. With this it is seen that

$$\chi^{-1}\mathrm{X}_1\chi = \mathrm{X}_1. \tag{11}$$

Suppose next that χ_0 is a substitution of X, such that

$$\tilde{\omega}/\chi_0 \equiv \gamma^{\lambda_0}\tilde{\omega} \pmod{\mathfrak{P}^2}, \tag{12}$$

where the exponent λ_0 has the least possible *positive* value that is not zero.

Then for every exponent a it follows from (8) and (9) that

$$\tilde{\omega}/\chi\chi_0^{-a} \equiv \gamma^{\lambda - a\lambda_0}\tilde{\omega} \pmod{\mathfrak{P}^2}.$$

Then, by a well known method, it may be shown that λ is divisible by λ_0 and is equal to $a\lambda_0$; and that is $\chi\chi_0^{-a}$ belongs to X_1. It follows that, if χ_1 is a substitution of X_1,

$$\chi = \chi_1\chi_0^a$$

for every χ of X. Accordingly, if h is the least positive exponent for which χ_0^h is an element of X_1, we have

$$\mathrm{X} = \mathrm{X}_1 + \mathrm{X}_1\chi_0 + \mathrm{X}_1\chi_0^2 + \cdots + \mathrm{X}_1\chi_0^{h-1}. \tag{13}$$

Due to (11) we may write also

$$\mathrm{X} = \mathrm{X}_1 + \chi_0\mathrm{X}_1 + \chi_0^2\mathrm{X}_1 + \cdots + \chi_0^{h-1}\mathrm{X}_1. \tag{14}$$

The degree of X is

$$g = hg_1. \tag{15}$$

From the meaning of h it is seen, if χ_0^k is an element in X_1 for any positive exponent k, that k must be divisible by h. It follows from (9) and the Fermat Theorem that for every element χ of X

$$\tilde{\omega}/\chi^{P^f-1} \equiv \gamma^{\lambda(P^f-1)}\tilde{\omega} \equiv \tilde{\omega} \pmod{\mathfrak{P}^2}.$$

With this it is seen that h is a divisor of $P'-1$, and therefore h is not divisible by p.

With this is proved the following: *The branch-group* X_1 *is a normal divisor of the inertia group* X. *Its degree* g_1 *is the highest power of* p, *see* (15), *that divides* g *and the group* X/X_1 *is cyclic of degree* h, *where* h *is a divisor of* $P'-1$.

It has been seen in Art. 233, that every integer Ω of $\mathfrak{R}$ is congruent, modulo $\mathfrak{P}$, to an integer Ω_0 of the inertia realm. Accordingly we may determine an integer τ, such that

$$\Omega-\Omega_0\equiv\tau\tilde{\omega}\ (\mathrm{mod.}\ \mathfrak{P}^2); \tag{16}$$

and as $\Omega_0/\chi=\Omega_0$ (since Ω_0 belongs to the inertia realm), it follows for every substitution χ_1 of X_1 due to (5), that

$$\Omega/\chi_1-\Omega_0\equiv\tau\tilde{\omega}\ (\mathrm{mod.}\ \mathfrak{P}^2), \tag{17}$$

and consequently due to (16) for every Ω in $\mathfrak{O}$, we have

$$\Omega/\chi_1\equiv\Omega\ (\mathrm{mod.}\ \mathfrak{P}^2). \tag{18}$$

Reciprocally, any substitution χ_1, which satisfies the condition (18) for every Ω, fulfills the requirement (2) and consequently belongs to the branch-group; and if application of this is made to the basis form β (Art. 230) of $\mathfrak{O}$, we may say: *The branch-group* X_1 *is also defined through the congruence*

$$\beta/\chi_1\equiv\beta\ (\mathrm{mod.}\ \mathfrak{P}^2).$$

Since g and therefore also g_1 is always a divisor of n, the degree of the realm, it is seen that X_1 is a unit group, if n is not divisible by p.

The realm $\mathfrak{R}_{\chi_1}$, which belongs to the branch-group X_1, is a divisor of $\mathfrak{R}$ above $\mathfrak{R}_\chi$, and from (14) the realm $\mathfrak{R}_{\chi_1}$ is relatively cyclic of degree h with respect to $\mathfrak{R}_\chi$.

To apply the theorems of Art. 232, we must replace the realms

$$\mathfrak{R},\ \mathfrak{R}',\ \mathfrak{k} \qquad \text{by} \qquad \mathfrak{R},\ \mathfrak{R}_{\chi_1},\ \mathfrak{R}_\chi,$$

and consequently the groups Φ and Φ' by X and X_1. We thus have $n=g$, $n'=g_1$. The formula (1), Art. 232, namely $n=n'm'$, becomes here $g=g_1m'$, which compared with (15) of Art. 234 gives $m'=h$. From (5), Art. 231, namely $n=efg$, we have here $g=efg$, so that $e=1=f$. From (4), Art. 231 and (6), Art. 232 it is seen that $g_r=g_1$, $e_r=1$; and from (5) and (7), Art. 232, $h_r=g_1$, $a_r=h$. Hence from (3) and (6) of Art. 232 it is seen that, $\mathfrak{p}'''$ denoting a prime ideal in the realm $\mathfrak{R}_{X_1}$, we have

$$\mathfrak{p}'''=\mathfrak{P}^{g_1}, \tag{19}$$

and in the realm $\mathfrak{R}_X$

$$\mathfrak{p}''=\mathfrak{p}'''^{h}. \tag{20}$$

With this is proved the theorem:

THEOREM. *The branch realm is relatively cyclic and of degree h with respect to the inertia realm. In the branch realm $\mathfrak{P}^{g_1}$ is a prime ideal, whose hth power is a prime ideal in the inertia realm.*

ART. **235. The Higher Branch Realms.** Under certain conditions there are still further groups contained in the branch-group X_1. These are called *higher branch-groups*, and they give rise to the higher branch realms.

We may define the *rth branch-group* X_r *as the complex of all the substitutions* χ_r, *which satisfy the condition*

$$\beta/\chi_r\equiv\beta \pmod{\mathfrak{P}^{r+1}}, \tag{1}$$

where β *is the basis form of* $\mathfrak{D}$.

Each of the groups X_r is contained in all the preceding groups $X_1, X_2, \cdots, X_{r-1}$, whose degrees are powers of p.

It may be that several of the groups $X_1, X_2, \cdots$ are identical. However eventually the unit group must appear in the series.

Instead of the *integer* $\tilde{\omega}$ of the preceding article, we must now employ a *form* $\tilde{\omega}$, whose content is a prime ideal in $\mathfrak{R}$ and this form $\tilde{\omega}$ here takes the place of the

integer $\tilde{\omega}$ which was divisible by the prime ideal $\mathfrak{P}$. From (1) it follows that for every integer and for every integral ideal $\mathfrak{J}$ of $\mathfrak{K}$ that

$$\mathfrak{J}/\chi_r \equiv \mathfrak{J} \pmod{\mathfrak{P}^{r+1}}, \tag{2}$$

and also that

$$\tilde{\omega}/\chi_r \equiv \tilde{\omega} \pmod{\mathfrak{P}^{r+1}}.$$

The latter congruence in the form of an equation is

$$\tilde{\omega}/\chi_r = \tilde{\omega} + \mathfrak{J}\tilde{\omega}^{r+1}. \tag{4}$$

This expression raised to any power ν, is

$$\tilde{\omega}^{\nu}/\chi_r \equiv \tilde{\omega}^{\nu} \pmod{\mathfrak{P}^{r+2}}. \tag{5}$$

Due to (1) we may write, if $\mathfrak{A}$ is an integral ideal,

$$\beta/\chi_r \equiv \beta + \mathfrak{A}\tilde{\omega}^{r+1} \pmod{\mathfrak{P}^{r+2}}. \tag{6}$$

If χ_r' is a second substitution of the group X_r and if

$$\beta/\chi_r' = \beta + \mathfrak{A}'\tilde{\omega}^{r+1} \pmod{\mathfrak{P}^{r+2}},$$

it follows from (6) that

$$\beta/\chi_r\chi_r' \equiv \beta + (\mathfrak{A}+\mathfrak{A}')\tilde{\omega}^{r+1} \pmod{\mathfrak{P}^{r+2}}, \tag{7}$$

and in general if a is a positive integer,

$$\beta/\chi_r^a \equiv \beta + a\mathfrak{A}\tilde{\omega}^{r+1} \pmod{\mathfrak{P}^{r+2}}. \tag{8}$$

Writing $a=p$ in this congruence, it is seen that χ_r^p is a substitution of X_{r+1}. Writing $a=-1$, which is of the same significance as $a=g_r-1$, it is seen that

$$\beta/\chi^{-1} \equiv \beta - \mathfrak{A}\tilde{\omega}^{r+1} \pmod{\mathfrak{P}^{r+2}}. \tag{9}$$

If $\chi_r = \chi_{r+1}$ is a substitution of the group X_{r+1}, we must put $\mathfrak{A}=0$ in (6), and then from (7) and (9) it follows that

$$\beta/\chi_r^{-1}\chi_{r+1}\chi_r \equiv \beta \pmod{\mathfrak{P}^{r+2}},$$

and therefore

$$\chi_r^{-1}\chi_{r+1}\chi_r = \chi_{r+1}', \tag{10}$$

where χ_{r+1}' is a substitution of X_{r+1}.

From (7) it is further seen for any two substitutions χ_r and χ'_r that

$$\beta/\chi_r\chi'_r \equiv \beta/\chi'_r\chi_r \pmod{\mathfrak{P}^{r+2}}; \tag{11}$$

and accordingly, if χ_{r+1} is a substitution of X_{r+1},

$$\chi_r\chi'_r = \chi'_r\chi_r\chi_{r+1}. \tag{12}$$

It is seen from formulas (10) and (12) that *the group* X_{r+1} *is a normal divisor of* X_r, *and that the group* $\mathrm{X}_r/\mathrm{X}_{r+1}$ *is commutative.*

If we form the branch realms $\mathfrak{R}_{\mathrm{X}_{r+1}}$, $\mathfrak{R}_{\mathrm{X}_r}$, it follows from induction (see Art. 232) by putting X_r and X_{r+1} in the place of Φ and Φ', *that in the rth branch realm* $\mathfrak{P}^{g_r}$ *is a prime ideal.*

In the following series of realms it is seen that each one contains the preceding together with their respective prime ideals which are divisible by $\mathfrak{P}$:

$$\begin{array}{llllllll} \mathfrak{k}, & \mathfrak{R}_\Psi, & \mathfrak{R}_{\mathrm{X}}, & \mathfrak{R}_{\mathrm{X}_1}, & \mathfrak{R}_{\mathrm{X}_2}, & \cdots, & \mathfrak{R}, \\ \mathfrak{p}, & \mathfrak{P}^g, & \mathfrak{P}^g, & \mathfrak{P}^{g_1}, & \mathfrak{P}^{g_2}, & \cdots, & \mathfrak{P}. \end{array} \tag{13}$$

This series is to be continued until the degree g_r of X_r is equal to 1; and then $\mathfrak{R}_{\mathrm{X}_r} = \mathfrak{R}$.

If g is not divisible by p, we have at once $\mathfrak{R}_{\mathrm{X}_1} = \mathfrak{R}$. We thus have the following noteworthy result:

Every realm $\mathfrak{R}$ *is relatively metacyclic with respect to the reduction (separation) realm of any prime ideal that is contained in it.*

Note. A realm, like a group, which has a series of indices that are prime integers, or powers of a prime, was called by Kronecker metacyclic.[1]

ART. 236. **Factorization of the Fundamental Ideal.** We may next determine the exponent of the highest

[1] They were called *solvable groups* by Frobenius and Hölder. See Vol. I, Art. 84 of the present treatise. See C. Jordan, *Traité des substitutions*, Livre IV.

power, to which a prime ideal $\mathfrak{P}$ appears as a divisor of the fundamental ideal $\mathfrak{G}_t$ of the realm $\mathfrak{R}$ with respect to $\mathfrak{k}$.

As seen in Art. 230 this fundamental ideal is had from the form

$$(1) \qquad f'(\beta)=(\beta-\beta^{(1)})(\beta-\beta^{(2)})\cdots(\beta-\beta^{(n-1)}),$$

where $\beta^{(1)}, \beta^{(2)}, \cdots, \beta^{(n-1)}$ are the conjugates of β. One of the factors of this product $\beta-\beta/\varphi$ is divisible by $\mathfrak{P}$ when and only when φ belongs to the inertia group, see Art. 231, (8). Since the identical substitution is excluded from this discussion, it follows that $\mathfrak{G}_t$ contains the factor $\mathfrak{P}$ at least $g-1$ times. Further $\beta-\beta/\chi$, is divisible by $\mathfrak{P}^2$ when and only when χ is an element of the branch-group X_1, and consequently $\mathfrak{G}_t$ is divisible by $\mathfrak{P}^{g-1+g_1-1}$ where $\mathfrak{P}$ is only counted to the g_1-1 power for the branch-group, it having been already counted $g-1$ times for the inertia group. Continuing we may determine the exact power of $\mathfrak{P}$ that divides $\mathfrak{G}_t$. It has the exponent

$$g-1+g_1-1+g_2-1+\cdots.$$

The g's are powers of p, whose exponents are not increasing and whose last exponent is 1.

It is thus seen that the composition of the fundamental ideal $\mathfrak{G}_t$ is completely determined through the separation of the group X.

The integers $g, g_1, g_2, \cdots$ are the same for all the conjugate ideals $\mathfrak{P}_1, \mathfrak{P}_2, \cdots, \mathfrak{P}_e$; and, if we write, Art. 231,

$$\mathfrak{p}=(\mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_e)^g,$$

it is seen that

$$(2) \qquad \mathfrak{G}_t=\Pi(\mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_e)^{g-1+g_1-1+g_2-1+\cdots},$$

where the product Π is to be taken over all the prime ideal factors of all the prime integers p in $\mathfrak{R}$. Observe that there are only a finite number of these prime integers p for which $g>1$. Note also that g is the number of elements χ in X and that $\mathfrak{P}/\chi=\mathfrak{P}$.

For the partial discriminant of the realm $\mathfrak{R}$ with respect to $\mathfrak{k}$ it results that [see (5), Art. 231]

$$\mathfrak{D}_t = \Pi \mathfrak{p}^{ef(g-1+g_1-1+g_2-1+\cdots)}; \tag{3}$$

and if R is the realm of rational numbers, so that $\mathfrak{p}$ becomes p, then $\mathfrak{D}_t$, neglecting sign, becomes the basal invariant (discriminant) D of the realm $\mathfrak{R}$, having the value

$$\pm D = \Pi p^{ef(g-1+g_1-1+g_2-1+\cdots)}, \tag{4}$$

where e is the number of ideal factors $\mathfrak{P}$ of $\mathfrak{p}$,

f is the degree of $\mathfrak{P}$ in $\mathfrak{k}$,

g is the degree of the inertia group,

g_1 that of the branch-group, etc.

Remark. The results here, due for the most part to Weber, *Algebra*, Vol. II, p. 671, are to be compared with those of Hensel given in Art. 256, end. And the two methods of derivation are to be studied in juxtaposition.

CHAPTER XV

THE GALOIS REALMS OF RATIONALITY

ART. 237. The Galois realms have the remarkable property that on the one hand the theory of ideals, which is associated with such realms, may be regarded as a special case of the general theory of ideals as treated in the previous chapters; and on the other hand the general treatment of ideals may be developed from the arithmetic of the Galois realms. For let $\mathfrak{k}$ be an arbitrary realm of rationality and form the Galois realm, which is the product of $\mathfrak{k}$ and its conjugate realms (Vol. I, Art. 53). Then necessarily the properties of $\mathfrak{k}$ have their source in the Galois realm and $\mathfrak{k}$ is a sub-realm of the Galois realm. (See Hensel, *Theorie der algebraischen Zahlen*, Chapt. XII.)

The peculiar property of the Galois realm, in that it is identical with its own conjugate realms, has as a consequence that the fundamental properties of the ideal theory may be proved much more simply; and its arithmetic may be much more easily developed than in the case of the general realms of rationality. It may therefore be taken—as Kronecker has in part done in his exposition of the theory [1]—as the foundation of the general arithmetic of the algebraic realms of rationality. At the same time [2] the knowledge of the arithmetical laws of the Galois realm, although not essential, is

[1] Kronecker, *Grundzüge*, pp. 10 et seq.; *Werke*, Vol. II, pp. 256 et seq.; see also Runge, *Crelle*, Vol. 99, pp. 89 et seq.

[2] The present chapter is, in a great measure, due to Bachman. See his *Allgemeine Arithmetik der Zahlenkörper*, Chap. XII; and this in turn is due to Hilbert, *Bericht*, pp. 247 ff., who originated much of this theory.

nevertheless useful for the full understanding of those of other special realms, for example the cyclotomic realms.

To develop the fundamental algebraic properties of the Galois realms, let $\mathfrak{R} = \mathfrak{R}(\mathrm{A})$ denote such a realm, and let A be an algebraic integer through which this realm is determined. Further let

$$F(x) = 0 \tag{1}$$

be an irreducible equation of the Nth degree, of which A is a root.

In Vol. I, Art. 44 it was seen that every number of $\mathfrak{R}$ was an integral function of A of degree at most equal to $N-1$ with rational coefficients that belonged to the stock-realm. We have the realms conjugate to $\mathfrak{R}$, if in these functions of A we replace A by its conjugate values. Since the conjugate realms of the Galois realm are in their totality identical with it, each realm having the same complex of numbers, it follows that each root of (1) is a rational function of any arbitrary root of this equation. (Arts. 210, 213.)

Any equation (1), whose roots may be expressed rationally through any one of them, is called a Galois equation and on this account the corresponding realm $\mathfrak{R}$ is called a *Galois realm*. Dedekind used the terminology *normal realm* (Dirichlet-Dedekind, *Zahlentheorie*, 4th Edition, p. 485).

The N roots of equation (1) may be denoted by

$$A, A^{(1)}, A^{(2)}, A^{(3)}, \cdots, A^{(N-1)}. \tag{2}$$

It follows that for $i = 1, 2, 3, \cdots, N-1$, we have

$$A^{(i)} = f_i(A), \tag{3}$$

where f_i is an integral function of A of degree at most equal to $N-1$, and with rational coefficients.

The substitutions through which the realm $\mathfrak{R}$ is transformed into its conjugate realms, that is, into the

realms which in the complex of numbers is identical with $\mathfrak{R}$, may be denoted by (Art. 211)

$$s_0, s_1, s_2, \cdots, s_{N-1} \qquad (=G), \tag{4}$$

where s_0 is the identical substitution which leaves $\mathfrak{R}$ unchanged. Denote these N substitutions, taken collectively, by G.

If $s_i\gamma$ is the number which γ becomes, when operated upon by the substitution s_i, then $s_iA = A_i$ and consequently

$$s_iA = f_i(A) \qquad (i=1, 2, \cdots, N-1). \tag{5}$$

If by the substitution s_1, the realm $\mathfrak{R}$ becomes another realm, and if this realm by the substitution s_2 becomes a third realm, then this third realm determines a substitution of the first realm, which substitution is said to be *compounded* out of s_1 and s_2, and is sometimes called the *product* $s_1 \cdot s_2$ of these substitutions. It does *not* follow that $s_2 \cdot s_1 = s_1 \cdot s_2$.

The N substitutions (4) form a group (Art. 212); that is, the product of any two of them $s_i \cdot s_k$ (including the case $i=k$) is one of the substitutions of (4). For the substitution s_i transforms the realm $\mathfrak{R}$ into another realm which consists of the same numbers as are in $\mathfrak{R}$, and the numbers of the second realm are rational functions of A. Hence the substitution s_k of the realm $\mathfrak{R}$ also denotes a substitution of the transformed realm. It is seen that the product s_ks_i of the two substitutions of $\mathfrak{R}$ is a substitution of $\mathfrak{R}$. Therefore, if we write

$$s_ks_i = s_h, \tag{6}$$

it follows, due to (5), since

$$s_ks_iA = s_kf_i(A) = f_is_k(A) = f_if_k(A),$$

that

$$f_if_k(A) = f_h(A). \tag{7}$$

In other words: s_i operating on $\Re(A)$ produces $\Re(A^{(i)}) = \Re(A)$; and that is

$$s_i\Re(A) = \Re(A^{(i)}) = \Re(A).$$

It follows that

$$s_k s_i \Re(A) = s_k \Re(A) = \Re(A^{(k)}) = \Re(A),$$

and consequently $s_k s_i \Re(A)$ is one of the N conjugate values,

$$s_0\Re(A),\ s_1\Re(A),\ \cdots,\ s_{N-1}\Re(A),$$

say

$$s_k s_i \Re(A) = s_h \Re(A),$$

or

$$s_k s_i = s_h.$$

From the composition of any two of the substitutions (4) arises the concept of the power s_i^m, as the mth repetition of the substitution s_i. (Art. 212.)

The Galois equation (1) is, in particular, an *Abelian equation*, if the relationship expressed through (7) is independent of the sequence of the operations f_i and f_k; that is, if (Art. 226)

$$f_i(f_k(A)) = f_k(f_i(A)). \tag{8}$$

And this implies also that

$$s_k s_i = s_i s_k. \tag{9}$$

This further implies the *commutative principle* for the substitutions of the group (4). Accordingly the *Galois realms of rationality* are the *Abelian realms*, if the substitutions of its group are *commutative*.

For the Abelian groups there exist the important theorem of Kronecker (Art. 159) namely: all the substitutions of the group may be expressed through products of powers of certain fundamental substitutions, $s_1, s_2, \cdots, s_\sigma$ in the form

$$s_1^{x_1} s_2^{x_2} \cdots s_\sigma^{x_\sigma}, \tag{10}$$

where in general x_i takes on the values $0, 1, \cdots, h_i - 1$

$(i=1, 2, \cdots, \sigma)$, subject to the condition that

$$N=h_1h_2\cdots h_\sigma.$$

The substitutions

$$s_i^0(=s_0=1),\ s_i^1,\ s_i^2,\ \cdots,\ s_i^{h_i-1}$$

form a sub-group of G, which on account of its peculiar character in that $s_i^{h_i}=s_i^0$ is called a *cyclic* group. It follows that an Abelian realm may be composed of a number of cyclic groups, whose degree—that is, the number of substitutions in such groups—may be assumed to be a prime number. (Art. 227.)

If the group of the Abelian realm is itself cyclic, the Abelian realm is in particular a cyclic realm. (See Art. 227.)

All these concepts, which hitherto in absolute sense have been defined for the realm $\mathfrak{R}$, whose stock-realm has been R, the realm of rational numbers, may be extended also to the more general case where the stock-realm is an arbitrary sub-realm $\mathfrak{k}$ of $\mathfrak{R}$, this latter realm being therefore a *relative realm* with regard to $\mathfrak{k}$.

Accordingly, a realm $\mathfrak{R}$ is called a *relative Galois realm* with respect to one of its sub-realms $\mathfrak{k}$, if the irreducible equation that is satisfied by A,

$$(11)\qquad x^r+k_1(\alpha)x^{r-1}+k_2(\alpha)x^{r-2}+\cdots+k_r(\alpha)=0,$$

where the coefficients are quantities of $\mathfrak{k}$, is a Galois equation. Here the number A is the algebraic quantity which determines $\mathfrak{R}$. This Galois equation is such that all the roots may be expressed as rational functions of one of them with coefficients that belong to $\mathfrak{k}$. (Art. 210.)

Denote by

$$(12)\qquad s_0,\ s_1,\ s_2,\ \cdots,\ s_{r-1}$$

the substitutions through which the realm $\mathfrak{R}$ is transformed into its relative conjugate realms and observe that these substitutions are the ones that leave the

coefficients in (11) unchanged. They have no effect on the numbers of $\mathfrak{k}$. These substitutions form a group which is called the *relative group*. If this relative group is commutative or *cyclic* the realm $\mathfrak{R}$ is said to be a *relative Abelian* or a *relative cyclic* realm.

ART. **238.** To establish in a simple manner the ideal theory of the Galois realms, it is proved below, as has already been done in the general case (Art. 14), that corresponding to every ideal of the Galois realm another ideal of this realm may be definitely determined, such that the product of the two ideals is a principal ideal.[1]

Let $\mathfrak{J}=(\Omega_1, \Omega_2, \cdots, \Omega_N)$ be an ideal of the realm $\mathfrak{R}$, whose degree is N. The ideal $\mathfrak{J}'$ is said to be *divisible* by the ideal $\mathfrak{J}$, and is written $\mathfrak{J}' \equiv 0 \pmod{\mathfrak{J}}$, if $\mathfrak{J}'=B_1\Omega_1 + B_2\Omega_2 + \cdots + B_N\Omega_N$, where the B's are quantities of $\mathfrak{R}$. Denote by G the substitution group of the realm $\mathfrak{R}$. (Art. 214.) An ideal $\mathfrak{J}$ is said to be *invariantive*,[2] if it remains unchanged, when subjected to the substitutions of the group G; that is, if the conjugate values of $\mathfrak{J}$ are all equal. Such an ideal has the following property.[3]

The $N!$ power of an invariantive ideal is always equal to a rational integer; that is

$$\mathfrak{J}^{N!}=\mathfrak{O}t, \tag{13}$$

where t is a rational integer and $\mathfrak{O}$ denotes the complex of integers of $\mathfrak{R}$.

To prove this, observe that every integer α of the ideal $\mathfrak{J}$ satisfies an equation of the Nth degree

$$\alpha^N + a_1\alpha^{N-1} + a_2\alpha^{N-2} + \cdots + a_N = 0, \tag{14}$$

where the a's are rational integers. Hence also

$$a_1^{N!},\ a_2^{\frac{N!}{2}},\ a_3^{\frac{N!}{3}},\ \cdots,\ a_N^{\frac{N!}{N}} \tag{15}$$

[1] See Hilbert, *Math. Ann.*, Vol. 44, p. 1.
[2] Hilbert, *Bericht*, § 57, uses the word "*ambiguous.*"
[3] Hilbert, *Bericht*, p. 248.

are rational integers. Denote their greatest common divisor by a. In like manner for all the integers β, γ, $\delta \cdots$ of the ideal determine the greatest common divisors $b, c, d, \cdots$, which are associated with them as above, and let t be the greatest common divisor of $a, b, c, \cdots$. Next note that, on the one hand, the numbers conjugate to α are again numbers of the ideal $\mathfrak{J}$, which is supposed invariantive; and on the other hand the coefficients of (14) are homogeneous integral functions of the quantities that are the conjugates of α [*i.e.*, the other roots of the equation (14)]. In fact a_1 is of the first dimension in these quantities, while a_2 is of the second and a_N is of the Nth dimension. It follows that

$$a_1 \equiv 0 \text{ (mod. } \mathfrak{J}), \quad a_2 \equiv 0 \text{ (mod. } \mathfrak{J}^2), \quad \cdots, \quad a_N \equiv 0 \text{ (mod. } \mathfrak{J}^N).$$

It is evident that all the numbers of (15) are contained in the ideal $\mathfrak{J}^{N!}$.

Since a, the greatest common divisor of the quantities (15) is a linear function of these quantities with integral coefficients, it follows that a is divisible by $\mathfrak{J}^{N!}$, as are also $b, c, \cdots$, so that $t\mathfrak{O}$ is divisible by $\mathfrak{J}^{N!}$.

On the other hand since each of the integers (15) is divisible by their greatest common divisor a, and therefore also by t, we may write $a_i^{\frac{N!}{i}} = tb_i$, where b_i is a rational integer. It follows that $a_i = t^{\frac{i}{N!}} b_i^{\frac{i}{N!}} = t^{\frac{i}{N!}} \tau_i$, where τ_i is an algebraic integer satisfying the equation

$$x^{N!} - b_i^i = 0.$$

Accordingly, equation (14) takes the form

$$\alpha^N + \tau_1 t^{\frac{1}{N!}} \alpha^{N-1} + \tau_2 t^{\frac{2}{N!}} \alpha^{N-2} + \cdots + \tau_N t^{\frac{N}{N!}} = 0.$$

Writing $\alpha = t^{\frac{1}{N!}} \alpha_1$, this equation becomes

$$\alpha_1^N + \tau_1 \alpha_1^{N-1} + \tau_2 \alpha_1^{N-2} + \cdots + \tau_N = 0.$$

It follows that (Vol. I, Art. 87) α_1 is an algebraic integer. Similarly it is seen that the other quantities $\beta, \gamma, \delta, \cdots$, of the ideal may be written

$$\beta = t^{\frac{1}{N!}}\beta_1, \ \gamma = t^{\frac{1}{N!}}\gamma_1, \ \cdots.$$

Hence every integer ζ of the ideal $\mathfrak{J}^{N!}$ is of the form $t\tau_0$, where τ_0 is an algebraic integer. Since τ_0 is equal to an integer ζ of $\mathfrak{R}$ divided by t, it follows that τ_0 is a quantity of $\mathfrak{R}$ and being integral, is an integer of $\mathfrak{R}$.

Hence $\mathfrak{J}^{N!}$ is divisible by $\mathfrak{D}t$ and, as shown above, $\mathfrak{D}t$ is divisible by $\mathfrak{J}^{N!}$. It follows that

$$\mathfrak{J}^{N!} = \mathfrak{D}t.$$

Due to this theorem, it follows that:

Associated with every ideal $\mathfrak{J}$ of the Galois realm there exists a second ideal $\mathfrak{J}'$ such that $\mathfrak{J}\mathfrak{J}'$ is a principal ideal.

For if $\mathfrak{J}$ is an ideal of a Galois realm, then are also $s_1\mathfrak{J}, s_2\mathfrak{J}, s_3\mathfrak{J}, \cdots, s_{N-1}\mathfrak{J}$ ideals of this realm, and their product

$$(16) \qquad s_0\mathfrak{J}\cdot s_1\mathfrak{J}\cdot s_2\mathfrak{J}\cdot \cdots \cdot s_{N-1}\mathfrak{J}$$

is an *invariantive* ideal of this Galois realm. For observe that, if any substitution s_i of the group G is applied to this product, the N substitutions

$$s_is_0, \ s_is_1, \ s_is_2, \ \cdots, \ s_is_{N-1}$$

form again the substitutions of the group G. Hence the factors of (16) are changed only as to their sequence; and due to the preceding remarks the $N!$ power of this product is a principal ideal, that is,

$$\mathfrak{J}\cdot s_1\mathfrak{J}\cdot s_2\mathfrak{J}\cdot \cdots \cdot s_{N-1}\mathfrak{J}[s_0\mathfrak{J}\cdot s_1\mathfrak{J}\cdots s_{N-1}\mathfrak{J}]^{N!-1}$$

is a principal ideal.

It follows that

$$\mathfrak{J}' = s_1\mathfrak{J}\cdots s_{N-1}\mathfrak{J}[s_0\mathfrak{J}\cdot s_1\mathfrak{J}\cdots s_{N-1}\mathfrak{J}]^{N!-1}$$

is an ideal as required in the theorem.

ART. 239. The arithmetic of the Galois realm may, due to this theorem, be developed as it was in the general case of Arts. 79 ff.

In connection with the Hilbert work (*loc. cit.*) the following may be remarked:

Any given realm $\mathfrak{k}$ may be regarded as a sub-realm of a Galois realm, for example, the realm which is compounded of $\mathfrak{k}$ and its conjugate realms.

Let $\mathfrak{K}$ be a Galois realm of the Nth degree and let $\mathfrak{k}$ be a sub-realm of $\mathfrak{K}$, then with respect to $\mathfrak{k}$, $\mathfrak{K}$ is a relative realm of degree $r=\frac{N}{n}$, where n is the degree of $\mathfrak{k}$.

The realm $\mathfrak{K}$ is produced by a quantity A which satisfies an equation of the form (11) so that $\mathfrak{K}=\mathfrak{R}(A)$.

The substitutions of the relative realm, namely, those which change A into its relative conjugates, that is, into the other roots of (11), are the substitutions of the original group G which leaves unchanged the numbers α of the sub-group $\mathfrak{k}$; and as $\mathfrak{k}=\mathfrak{R}(\alpha)$, all the numbers of $\mathfrak{k}$ remain unchanged by such substitutions. These substitutions may be denoted by

$$s_0,\ s_1,\ s_2,\ \cdots,\ s_{r-1} \tag{17}$$

They form a group which due to the fact that they are to be found among the substitutions of the group G, is called a sub-group of G. It is clear that the equation (11) is a Galois equation, since its roots are certain of the roots of equation (1). They may be expressed, therefore, through one another, so that the relative conjugate realms of the relative realm $\mathfrak{K}$ are identical with it.

Let $\mathfrak{i}$ be an ideal of $\mathfrak{k}$, say

$$\mathfrak{i}=(\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_\mu)$$

or

$$\mathfrak{i}=\alpha_1\gamma_1+\alpha_2\gamma_2+\cdots+\alpha_\mu\gamma_\mu,$$

where $\gamma_i (i=1,\ 2,\ \cdots,\ \mu)$ are integers of $\mathfrak{k}$.

Since the numbers $\alpha_1, \alpha_2, \cdots, \alpha_\mu$ are also quantities of $\mathfrak{R}$, it is clear that numbers of the form

$$\alpha_1\Gamma_1+\alpha_2\Gamma_2+\cdots+\alpha_\mu\Gamma_\mu, \quad \text{where} \quad \Gamma_i(i=1, \cdots, \mu)$$

are quantities of $\mathfrak{R}$, form an ideal of $\mathfrak{R}$, which may be denoted by

$$\mathfrak{J}=(\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_\mu).$$

Accordingly, there corresponds to every ideal $\mathfrak{i}$ of the sub-realm an ideal $\mathfrak{J}$ of the super-realm, where the two ideals may be regarded as of the same significance; that is, if $\mathfrak{O}$ denotes the complex of all integers of $\mathfrak{R}$, then is

$$\mathfrak{J}=\mathfrak{O}\mathfrak{i}.$$

Suppose next that $\mathfrak{B}$ is an ideal of the Galois realm such that

$$\mathfrak{J}\mathfrak{B}=\mathfrak{O}\Omega \tag{18}$$

is a principal ideal, and that is, Ω is an algebraic integer of $\mathfrak{R}$. It follows that

$$s_0\Omega=\Omega=\alpha_1\beta_1+\alpha_2\beta_2+\cdots+\alpha_\mu\beta_\mu,$$

where $\beta_1, \beta_2 \cdots \beta_\mu$ are integers belonging to the ideal $\mathfrak{B}$.

Since the substitutions of (17) leave the α's unchanged, it is seen that

$$\begin{aligned}
s_1\Omega&=\alpha_1 s_1\beta_1+\alpha_2 s_1\beta_2+\cdots+\alpha_\mu s_1\beta_\mu,\\
s_2\Omega&=\alpha_1 s_2\beta_1+\alpha_2 s_2\beta_2+\cdots+\alpha_\mu s_2\beta_\mu,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
s_{r-1}\Omega&=\alpha_1 s_{r-1}\beta_1+\alpha_2 s_{r-1}\beta_2+\cdots+\alpha_\mu s_{r-1}\beta_\mu.
\end{aligned}$$

If we multiply these expressions together and put

$$s_0\Omega s_1\Omega \cdots s_{r-1}\Omega=\overline{\Omega},$$

it is clear that

$$\overline{\Omega}=\alpha_1^r B_1+\alpha_1^{r-1}\alpha_2 B_2+\cdots+\alpha_\mu^r B_\nu, \tag{19}$$

where ν denotes the number of all possible products of the rth dimension that can be made from $\alpha_1, \alpha_2 \cdots \alpha_\mu$, while the quantities B_i are symmetric functions of $\beta_1, \beta_2, \cdots, \beta_\mu$.

Since these symmetric functions remain unchanged when subjected to the substitutions (17), it is seen that $B_i (i=1, \cdots, \nu)$ are integers of $\mathfrak{k}$. The same is therefore true of $\overline{\Omega}$; and consequently, due to (19), it is seen that $\overline{\Omega}$ is contained in the ideal

$$\mathfrak{i}^r(B_1, B_2, \cdots, B_\nu) \tag{20}$$

of the realm $\mathfrak{k}$. On the other hand it follows from (18) that each of the numbers α_i when multiplied by every number of $\mathfrak{B}$ is divisible by Ω, and in particular $\alpha_i\beta_i$ is divisible by Ω. Therefore every product of r numbers α_i by one of the numbers of B_i, due to the manner in which B_i is formed, is an algebraic integer of $\mathfrak{k}$, which is divisible by $\overline{\Omega}$. Hence the ideal (20) is contained in $\mathfrak{o}\overline{\Omega}$, where $\mathfrak{o}$ denotes the complex of the integers of $\mathfrak{k}$. This, in connection with the results previously obtained, proves the relation

$$\mathfrak{o}\overline{\Omega} = \mathfrak{i}^r(B_1, B_2, \cdots, B_\nu);$$

and that is:

Associated with any arbitrary ideal $\mathfrak{i}$ *of* $\mathfrak{k}$ *there is another ideal* $\mathfrak{i}^{r-1}(B_1, B_2, \cdots, B_\nu)$ *of* $\mathfrak{k}$ *which, when multiplied by* $\mathfrak{i}$, *is a principal ideal of* $\mathfrak{k}$.

Thus by a simple consideration of the theory of the Galois realms the *primary* theorem has been proved, from which the entire arithmetic of an arbitrarily given realm $\mathfrak{k}$ may be developed, and in a manner similar to that previously done for the case of the general theory of ideals.

ART. **240.** The principal properties of the Galois realm may be developed through proofs of the following theorem:

The different $\mathfrak{D}$ *of the Galois realm* $\mathfrak{K}$ *is an invariantive ideal, and its discriminant* D (*or more exactly the principal ideal* $\mathfrak{O}D$) *is equal to* $\mathfrak{D}^N$.

Proof. Denote by $\Omega_1, \Omega_2, \cdots \Omega_N$ any basis of the Galois realm. Its elements are (see Art. 77) the ideals

$$(21)\quad \begin{cases} \mathfrak{F}^{(1)} = (\Omega_1 - s_1\Omega_1, & \Omega_2 - s_1\Omega_2, & \cdots, & \Omega_N - s_1\Omega_N), \\ \mathfrak{F}^{(2)} = (\Omega_1 - s_2\Omega_1, & \Omega_2 - s_2\Omega_2, & \cdots, & \Omega_N - s_2\Omega_N), \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \mathfrak{F}^{(N-1)} = (\Omega_1 - s_{N-1}\Omega_1, & \Omega_2 - s_{N-1}\Omega_2, & \cdots, & \Omega_N - s_{N-1}\Omega_N). \end{cases}$$

We saw (Art. 77) in the case of the general realm that these elements are not quantities of the realm, although their product is an ideal of such a realm. In the case of the Galois realm, however, the differences in (21) are all quantities of such a realm, the product of the $\mathfrak{F}$'s being the *different* (principal ideal) of the realm. It was proved (see Art. 106) that the *norm* of the *different* is equal to the discriminant of the realm.

Observe that if any substitution s_k of the group G is applied to $\mathfrak{F}^{(i)}$, this ideal becomes

$$(22)\qquad (s_k\Omega_1 - s_k s_i\Omega_1, \cdots, s_k\Omega_N - s_k s_i\Omega_N),$$

which also belongs to the Galois realm. Since, however,

$$(23)\qquad s_k s_i s_k^{-1} = s_i',$$

where s_i' is a definite substitution of the group G, it is seen that

$$s_k s_i = s_i' s_k.$$

It follows that the expression (22) becomes

$$(24)\qquad (s_k\Omega_1 - s_i' s_k\Omega_1, \cdots, s_k\Omega_N - s_i' s_k\Omega_N),$$

in which the numbers

$$(25)\qquad s_k\Omega_1, s_k\Omega_2, \cdots, s_k\Omega_N$$

form a basis of a realm that is conjugate to $\mathfrak{R}$, and that is to the Galois realm itself.

If s_i goes through all the substitutions of G, then will s_i' go through those substitutions. Consequently the prod-

uct of the elements (21) when i goes over the values 0, 1, $\cdots$, $N-1$, remains invariantive, and consequently we have $s_k\mathfrak{D}=\mathfrak{D}(k=0, 1, \cdots, N-1)$. It follows that

$$D=N(\mathfrak{D})=\mathfrak{D}^N.$$

ART. 241. The arithmetical as well as the algebraic properties of the Galois realm depend upon the relation in which this realm stands to the different sub-realms that are contained in it, as well as upon the manner in which these sub-realms stand to one another. It was remarked above that the substitutions of the group G of the Galois realm $\mathfrak{R}$, which do not change the numbers of one of its sub-realms $\mathfrak{k}$, themselves form a realm. Thus corresponding to every sub-realm $\mathfrak{k}$ of $\mathfrak{R}$ there is a definite sub-group g of G. It is clear that the inverse is also true; that is, to every sub-group g there belongs a definite sub-realm $\mathfrak{k}$ of the Galois realm; and in fact the complex of all the numbers of the Galois realm, which remain unchanged when subjected to the substitutions of g, constitute this sub-realm $\mathfrak{k}$. In this manner the *sub-realms of the Galois realm and the sub-groups of the Galois group are uniquely associated with one another.*

To develop the ideal theory of the Galois realm and its sub-realms, it is above all necessary to consider its prime ideals.

Let $\mathfrak{P}$ be any prime ideal of the realm $\mathfrak{R}$. Then among the substitutions of the group G there are always some, which when applied to $\mathfrak{P}$, leave unchanged the complex of numbers that are contained in $\mathfrak{P}$, when the sequence is neglected. For at all events the identical substitution s_0, which leaves unchanged all the numbers of $\mathfrak{R}$, is a substitution just described.

Denote the substitutions in question by

$$z_0(=s_0),\ z_1,\ z_2,\ \cdots$$

and let the number of them be r_z. It is evident that these substitutions form a group which may be denoted by g_z, and which Hilbert [1] has called the *separation* (*Zerlegungsgruppe*) *group* of the prime ideal $\mathfrak{P}$. The sub-realm that is associated with the group g_z, that is the complex of numbers in $\mathfrak{R}$ which remain unchanged when subjected to these substitutions is called the *separation realm* of the prime ideal $\mathfrak{P}$, and may be denoted by $\mathfrak{k}_z$. Its degree is $n_z = \frac{N}{r_z}$. Hence with respect to the separation realm, $\mathfrak{R}$ is a relative realm of degree r_z, there being, with respect to $\mathfrak{k}_z$, an integer A which generates $\mathfrak{R}$ and satisfies an irreducible equation of degree r_z in which the first coefficient is 1 and the other numbers are integral numbers of the realm $\mathfrak{k}_z$. (See Art. 233.)

The separation realm contains another realm which is of peculiar importance (see Hilbert, *Nach. der Gött. Ges.*, 1894–95, p. 224; and Dedekind, p. 272 of the same journal 1894–95). Hilbert called this sub-realm of $\mathfrak{R}$ the *inertia* realm of the prime ideal $\mathfrak{P}$ and its associated group the *inertia* group. This group and realm are defined below. (Also see Art. 233.)

The inertia group may be denoted by g_i, the number of its substitutions being indicated by r_i while the inertia realm may be denoted by $\mathfrak{k}_i$ being of degree $\frac{N}{r_i} = n_i$. Hence with respect to the inertia realm, the Galois realm $\mathfrak{R}$ is a relative realm of degree r_i.

The substitutions of the inertia realm may be defined as those substitutions of the Galois group G, say

$$t_0 (= s_0),\ t_1,\ t_2,\ \cdots,$$

which have the property that, when applied to every integer

[1] Hilbert, *Bericht*, p. 251.

Ω *of* $\mathfrak{K}$, *the congruence*

$$t_i\Omega \equiv \Omega \pmod{\mathfrak{P}} \tag{27}$$

exists.

It may be proved as follows that the substitutions t_i form a group. For from (27) it follows at once that, if Ω is divisible by $\mathfrak{P}$, then $t_i\Omega$ is also, and consequently the ideal $t_i\mathfrak{P}$ is contained in the ideal $\mathfrak{P}$. On the other hand since t_i belongs to the group G, it follows that t_i^{-1} is a substitution of this group. Hence $t_i^{-1}\Omega = \Omega'$, where Ω' is a number of $\mathfrak{K}$. It follows that $t_i\Omega' = \Omega$. Since $t\Omega' \equiv \Omega' \pmod{\mathfrak{P}}$, by definition of t_i, it follows that $\Omega \equiv \Omega' \pmod{\mathfrak{P}}$; and consequently Ω' at the same time with Ω is contained in $\mathfrak{P}$. It is seen that every number of the ideal $\mathfrak{P}$ is contained in $t_i\mathfrak{P}$. This with the preceding results shows that $t_i\mathfrak{P} = \mathfrak{P}$, and consequently the substitutions t_i are to be counted with those that leave the prime ideal unchanged. It follows at once that

$$t_k t_i \Omega \equiv t_k \Omega \equiv \Omega \pmod{\mathfrak{P}},$$

or the product of the two substitutions $t_k t_i$ belongs to the group g_i. From above it follows that this group is a sub-group of the separation group; and hence the separation realm is contained in the inertia realm.

ART. 242. To make clear the relations that exist between the separation group and the inertia group, let p be a rational prime integer which is divisible by $\mathfrak{P}$, so that (Art. 29)

$$\text{norm } (\mathfrak{P}) = p^f \text{ (in } \mathfrak{K}), \tag{28}$$

where f is the degree of $\mathfrak{P}$.

We may prove first that, *if* $f \neq 1$, *there is a substitution* z *of the separation group which is not found in the inertia group, such that* z^f *is a substitution of the inertia group, and that is*

$$z^f\Omega \equiv \Omega \pmod{\mathfrak{P}} \tag{29}$$

for every integer Ω *of* $\mathfrak{P}$.

To prove this let ρ be a primitive number (mod. $\mathfrak{P}$), which may be subjected to the condition that it is divisible by all the ideals that are conjugate to $\mathfrak{P}$ but not by $\mathfrak{P}$ itself. For we may always determine a number, which satisfies the congruences

$$\Omega \equiv 0 \pmod{\mathfrak{P}^{(1)}},\ \Omega \equiv 0 \pmod{\mathfrak{P}^{(2)}},\ \cdots,$$

and then choose a primitive number $\rho \equiv \Omega \pmod{\mathfrak{P}}$. Further observe that ρ, like any other integer of the realm $\mathfrak{R}$, satisfies an equation

$$\psi(x) = (x - s_0\rho)(x - s_1\rho)\cdots(x - s_{N-1}\rho). \tag{30}$$

Consider this equation as a congruence (mod. $\mathfrak{P}$). Since $[\psi(x)]^p \equiv \psi(x) \pmod{\mathfrak{P}} \equiv \psi(x^p)$ (Art. 30), it is evident that one of the quantities $s_0\rho, s_1\rho, \cdots, s_{N-1}\rho$ is congruent (mod. $\mathfrak{P}$) to ρ^p, say

$$s_i\rho \equiv \rho^p \pmod{\mathfrak{P}}. \tag{31}$$

This substitution belongs to the reduction group; for if $s_i\mathfrak{P}$ were *not* equal to $\mathfrak{P}$, and consequently if $s_i^{-1}\mathfrak{P}$ were not equal to $\mathfrak{P}$, then $s_i^{-1}\mathfrak{P}$ would be identical with one of the ideals that is conjugate to $\mathfrak{P}$ but different from $\mathfrak{P}$; and since, by hypothesis, ρ is divisible by this conjugate ideal, it would follow that $s_i\rho$ was divisible by $\mathfrak{P}$, which the congruence (31) does *not* permit.

Accordingly we may write for s_i the substitution z, so that

$$z\rho \equiv \rho^p \pmod{\mathfrak{P}}. \tag{32}$$

From this congruence follow at once

$$z^2\rho \equiv \rho^{p^2},\ z^3\rho \equiv \rho^{p^3},\ \cdots,\ z^f\rho \equiv \rho^p \pmod{\mathfrak{P}}.$$

But since ρ is a primitive number, it is seen that $\rho^p \equiv \rho$ (mod. $\mathfrak{P}$); and accordingly

$$z^f\rho \equiv \rho \pmod{\mathfrak{P}}. \tag{33}$$

From (32) and (33) it follows that the substitution z, if $f > 1$, is not a substitution of the inertia group, although

z^f is. Observe that every integer Ω of $\mathfrak{K}$ is either divisible by $\mathfrak{P}$ or it is congruent to a power of ρ (mod. $\mathfrak{P}$). In the first case, since Ω is a number of $\mathfrak{P}$, it follows from the definition of the separation group that $z\Omega \equiv \Omega$ (mod. $\mathfrak{P}$), and therefore also $z^f\Omega \equiv \Omega$ (mod. $\mathfrak{P}$); in the other case it follows from $\Omega \equiv \rho^i$ (mod. $\mathfrak{P}$) and (33) that

$$z^f\Omega \equiv z^f\rho^i \equiv (z^f\rho)^i \equiv \rho^i \equiv \Omega \text{ (mod. } \mathfrak{P}).$$

Hence in all cases

$$z^f\Omega \equiv \Omega \text{ (mod. } \mathfrak{P}).$$

It follows by definition of the group of substitutions t that z^f is one of these substitutions.

It may be proved secondly that all the substitutions of the separation group may be expressed through the following f complexes of substitutions, in each of which t goes through all of the substitutions of the inertia group; namely, through the complexes

$$t,\ zt,\ z^2t,\ \cdots,\ z^{f-1}t, \tag{34}$$

or using the Galois notation of Art. 220,

$$g_z = g_t + zg_t + \cdots + z^{f-1}g_t. \tag{35}$$

Proof. The primitive number ρ satisfies (Arts. 60, 72, 103) an irreducible integral congruence (mod. $\mathfrak{P}$) of the fth degree, say

$$F(x) \equiv 0 \text{ (mod. } \mathfrak{P}),$$

the other roots being

$$\rho,\ \rho^p,\ \rho^{p^2},\ \cdots,\ \rho^{p^{f-1}}.$$

Further observe that the integer $F(\rho)$, which satisfies the congruence

$$F(\rho) \equiv 0 \text{ (mod. } \mathfrak{P}),$$

is a number of the ideal $\mathfrak{P}$, and hence remains unchanged when operated upon by one of the substitutions of g_z, so that

$$F(z_i\rho) \equiv 0 \text{ (mod. } \mathfrak{P}).$$

Hence $z_i\rho$ is congruent to one of the roots $\rho, \rho^p, \cdots, \rho^{p^{f-1}}$, say

$$z_i\rho \equiv \rho^{p^k} \equiv z^k\rho \pmod{\mathfrak{P}};$$

that is

$$z^{-k}z_i\rho \equiv \rho \pmod{\mathfrak{P}}.$$

It follows at once as above that

$$z^{-k}z_i\Omega \equiv \Omega \pmod{\mathfrak{P}}.$$

Hence $z^{-k}z_i$ is one of the substitutions t of the inertia group, and we may write $z_i = z^k t$, a substitution, which is therefore to be found in one of the complexes (34). In this form all the substitutions $z_0, z_1, z_2, \cdots$ of the separation group may be expressed. On the other hand the substitutions $z^k t$, for $k = 0, 1, 2, \cdots, f-1$, are different from one another. It follows that the complexes (34) constitute all the substitutions of the separation group.

From (32) it is seen that

$$t_i z\rho \equiv t_i \rho^p \pmod{\mathfrak{P}},$$

where z is a definite substitution of the separation group, and t_i is any substitution of the inertia group. Due to the nature of the substitutions t_i, and since

$$t_i\rho^p \equiv \rho^p \pmod{\mathfrak{P}},$$

it follows that, if use is made of (32),

$$t_i z\rho \equiv z\rho, \qquad \text{or} \qquad z^{-1}t_i z\rho \equiv \rho \pmod{\mathfrak{P}}.$$

The more general congruence

$$z^{-1}t_i z\Omega \equiv \Omega \pmod{\mathfrak{P}}$$

is had for every integer Ω of $\mathfrak{R}$, if we observe that

$$\Omega \equiv \rho^h \pmod{\mathfrak{P}},$$

where h is a definite one of the integers $1, 2, \cdots, p^f - 1$. Hence $z^{-1}t_i z$ belongs to the inertia group.

Accordingly this group has the property, which may be expressed through the relation

(36) $$z^{-1}g_\iota z = g_\iota,$$

a property which may be characterized [1] *as the " invariance " of the inertia group.*

We may next give the rule by which the prime integer p may be distributed (decomposed) into its prime ideal factors in the Galois realm. Since g_z is a sub-group of the Galois group and as r_z is the degree of g_z, there exist in G (Arts. 214, 220) certain substitutions $s_0, s_1, \cdots, s_{n_z-1}$, such that the group G may be distributed into the complexes

$$s_0 g_z,\ s_1 g_z,\ \cdots,\ s_{n_z-1} g_z, \tag{37}$$

and that is

$$G = s_0 g_z + s_1 g_z + \cdots + s_{n_z-1} g_z. \tag{38}$$

To obtain all the prime ideals that are conjugate to $\mathfrak{P}$, observe that g_z when applied to $\mathfrak{P}$ leaves the ideal unchanged, so that each of the complexes (37) offers one ideal and only one, namely

$$s_0\mathfrak{P}(=\mathfrak{P}),\ s_1\mathfrak{P},\ \cdots,\ s_{n_z-1}\mathfrak{P}. \tag{39}$$

These are all different; for were $s_1\mathfrak{P} = s_2\mathfrak{P}$, it would follow that $s_1^{-1}s_2\mathfrak{P} = \mathfrak{P}$, and consequently $s_1^{-1}s_2$ would be one of the substitutions, say z_i of the group g_z. In that event, it would follow that $s_2 = s_1 z_i$ and that is s_2 is one of the substitutions of the complex $s_1 g_z$, which is in contradiction with the method by which these complexes were formed. Hence each of the prime ideals (39) exists through the application of the substitutions of G upon $\mathfrak{P}$ an equal number of times, that is r_z times, where r_z is the number of substitutions in each of the complexes (37).

The formula (28) accordingly offers the relation

$$p^f = (\mathfrak{P} \cdot s_1\mathfrak{P} \cdot \cdots \cdot s_{n_z-1}\mathfrak{P})^{r_z}.$$

Due to formula (35) it is seen that

$$r_z = f r_t, \tag{40}$$

[1] Hilbert, *Bericht*, p. 252.

and consequently,

$$p = (\mathfrak{P} \cdot s_1\mathfrak{P} \cdot \cdots \cdot s_{n_z-1}\mathfrak{P})^{r_t}, \tag{41}$$

which is the theorem[1] *required for the distribution of a rational prime integer into its prime ideal factors in* $\mathfrak{R}$.

ART. **243.** The next problem is to derive the prime ideal factors into which the rational prime integer p may be resolved in a sub-realm $\mathfrak{k}$ of $\mathfrak{R}$.

If n is the degree of $\mathfrak{k}$, then $\mathfrak{k}$ belongs to a sub-realm g of G, which contains $r = \frac{N}{n}$ substitutions, namely those which (Art. 239) do not change the numbers of $\mathfrak{k}$. To solve this problem we must determine the relations which exist among the sub-group g, the separation and inertia groups. The groups G and g will be distributed into certain complexes in the present article and we shall return to the further factorization of p in the following article.

Let s be a definite substitution of G, while z' denotes any substitution of g_z and s' any substitution of g. It follows that all substitutions of the form $s'sz'$ form a complex, which may be denoted by

$$gsg_z \tag{42}$$

and which contains rr_z substitutions. These substitutions are *not* all different. To prove this write

$$s'sz' = s''sz'', \tag{43}$$

where s'' and z'' are substitutions of g and g_z respectively.

It follows that

$$s''^{-1} \cdot s' = s(z''z'^{-1})s^{-1},$$

where $s''^{-1}s'$ is a substitution, s^0 say, of g, while $z''z'^{-1}$ is a substitution, z^0, of g_z. Accordingly, the two substitu-

[1] See Hilbert, "Theorie der algebraischen Zahlkörper," *Encyclopaedie der mathematischen Wissenschaften*, §§ 14, 15, pp. 688–690.

tions (43) of the complex (42) are equal, when and only when

$$s^0 = sz^0s^{-1}; \tag{44}$$

and that is, when this substitution, expressed in the two ways, is contained in the two groups g and $s \cdot g_z \cdot s^{-1}$. The substitutions which are common to the two groups form (Art. 220) a group which may be denoted by $\bar{g}$ of degree h. If $s'sz'$ is a substitution of the complex (42), there corresponds to each of the h substitutions of (44) another definite substitution $s''sz''$ of the same complex, where s'', z'' are determined through $s''^{-1}s' = s^0$, $z''z'^{-1} = z^0$ and where $s'sz' = s''sz''$. Accordingly *there are always, corresponding to any substitutions of the complex (42), $h-1$ substitutions of this complex which are equal to the first one; and consequently rr_z is a multiple of h.*

Observe that the substitutions of G may be distributed into a number of complexes of the form (42), if different substitutions are written for s. And [see (38)] these different substitutions need only be selected from the series

$$s_0, s_1, \cdots, s_{n_z-1}. \tag{45}$$

For, if we write s_1g_z for s in gsg_z, we have

$$gs_1g_zg_z = gs_1g_z.$$

Next observe, if s_i, s_k are any two of these substitutions, that the substitutions of gs_ig_z are either identical with those of gs_kg_z or they are all different, according as s_k is, or is not, a substitution of gs_ig_z. For, if s_k is a substitution of gs_ig_z, we would have $s_k = s's_iz'$, where s' is a substitution of g, and z' is a substitution of g_z. And in this case $gs_kg_z = gs's_iz'g_z$, where gs' is a substitution of g, and $z'g_z$ is a substitution of g_z. In the second case an equality of the form $s's_iz' = s''s_kz''$ cannot exist; for it would follow that $s_k = (s'')^{-1}s's_iz'z''^{-1}$, making s_k, con-

trary to the assumption, a substitution of the first complex. Accordingly we have all the substitutions of the group G if for a certain number, say e, of the substitutions of the series (45)—we may name them $s_0, s_1, \cdots, s_{e-1}$—, we make the complexes

$$(46) \qquad g s_0 g_z,\ g s_1 g_z,\ \cdots,\ g s_{e-1} g_z.$$

Further observe that the substitutions of the group G, according as they are found in the first, second, $\cdots$, or eth complex, enter respectively $h_0, h_1, \cdots, h_{e-1}$ times, where $h_i (i = 0, 1, \cdots, e-1)$ denotes the degree of the group $\bar{g}_i$, this being the group that contains the substitutions that are common to the two groups g and

$$s_i g_z s_i^{-1} = g_z^{(i)} \qquad (i = 0, 1, \cdots, e-1).$$

Finally note, since $\bar{g}_i$ is a sub-group of g, that g may be distributed into a certain number e_i of complexes of the form

$$(48) \qquad s' \bar{g}_i,\ s'' \bar{g}_i,\ \cdots,\ s^{(e_i)} \bar{g}_i,$$

where $s', s'', \cdots, s^{(e_i)}$ are defined as substitutions of g; or, using the Galois notation,

$$(49) \qquad g = s' \bar{g}_i + s'' \bar{g}_i + \cdots + s^{(e_i)} \bar{g}_i.$$

Finally observe that r, the degree of g, is the product of e_i and h_i, or

$$(50) \qquad r = e_i h_i.$$

ART. **244.** The results that have been established in the preceding article are sufficient for the derivation of everything that is essential to the factorization of the prime integer p into its prime ideal factors in the sub-realm $\mathfrak{k}$. To this end again let $\mathfrak{P}$ be a prime ideal factor of p in the realm $\mathfrak{R}$. This ideal has certain integers in common with the sub-realm $\mathfrak{k}$, and in particular it contains p, since every rational integer is contained in any realm above R. The collectivity of all these integers is

an ideal $\mathfrak{p}$ which in fact is a prime ideal factor of p in $\mathfrak{k}$. For observe that $\mathfrak{p}$ is an ideal in $\mathfrak{k}$ and that $\mathfrak{O}\mathfrak{p}$ is a complex of integers that are all found in $\mathfrak{P}$, so that $\mathfrak{O}\mathfrak{p}$ is divisible by $\mathfrak{P}$ or $\mathfrak{p}$ is divisible by $\mathfrak{P}$. Further $\mathfrak{p}$ is a prime ideal of $\mathfrak{k}$. For were this not the case, then we would have $\mathfrak{p} = \mathfrak{q} \cdot \mathfrak{r}$, where $\mathfrak{q}$ and $\mathfrak{r}$ are ideals in $\mathfrak{k}$. Hence also $\mathfrak{O}\mathfrak{q}$ and $\mathfrak{O}\mathfrak{r}$ are ideals in $\mathfrak{K}$, and since $\mathfrak{p}$ is divisible by $\mathfrak{P}$, it follows that either $\mathfrak{O}\mathfrak{q}$ or $\mathfrak{O}\mathfrak{r}$ is divisible by this prime ideal, say $\mathfrak{O}\mathfrak{q}$. Thus $\mathfrak{q}$ is contained in $\mathfrak{P}$; and since all the numbers common to $\mathfrak{P}$ and $\mathfrak{k}$ are contained in $\mathfrak{p}$ it is seen that $\mathfrak{q}$ is divisible by $\mathfrak{p}$; on the other hand, since $\mathfrak{p}$ is divisible by $\mathfrak{q}$, it is seen that $\mathfrak{p} = \mathfrak{q}$. It follows that *to every prime ideal factor $\mathfrak{P}$ of p in $\mathfrak{K}$ there corresponds a prime ideal factor $\mathfrak{p}$ of p in $\mathfrak{k}$, and $\mathfrak{p}$ is divisible by $\mathfrak{P}$.*

Reciprocally, there corresponds to every prime ideal factor of p in $\mathfrak{k}$ an ideal factor $\mathfrak{O}\mathfrak{p}$ in $\mathfrak{K}$, which is not necessarily a prime ideal in $\mathfrak{K}$. However, since $\mathfrak{p}$ contains the rational prime integer p, it is an ideal divisor of p and therefore $\mathfrak{O}\mathfrak{p}$ is divisible by at least one prime ideal factor $\mathfrak{P}$ of p in $\mathfrak{K}$.

Observe that $\mathfrak{P}$ and $\mathfrak{P}_1$ might both be divisors of $\mathfrak{O}\mathfrak{p}$, and while different they might, nevertheless, contain all integers of $\mathfrak{k}$ that are found in $\mathfrak{p}$. Now $\mathfrak{p}$ is the complex of integers that are common to $\mathfrak{k}$ and $\mathfrak{P}$; for were $\mathfrak{p}$ different from this complex, which we call $\mathfrak{p}'$, then $\mathfrak{p}$ would be contained in $\mathfrak{p}'$ and therefore divisible by $\mathfrak{p}'$. By hypothesis $\mathfrak{p}$ is a prime ideal in $\mathfrak{k}$, so that, if it is divisible by $\mathfrak{p}'$, it must be identical with it. The following has thus been proved:

Associated with every prime ideal factor $\mathfrak{p}$ of p in $\mathfrak{k}$ there is at least one prime ideal factor $\mathfrak{P}$ of p in $\mathfrak{K}$, in which $\mathfrak{p}$ is contained as the collectivity of integers that are common to $\mathfrak{k}$ and $\mathfrak{P}$.

We therefore may find all prime ideal factors $\mathfrak{p}$ of p in $\mathfrak{k}$ and only such, if for all prime ideal factors $\mathfrak{P}$ of p in $\mathfrak{K}$ we choose those which have in common the greatest number of integers of $\mathfrak{k}$.

Next we observe that, if $\mathfrak{P}$ is an ideal divisor of p in $\mathfrak{K}$, then are $s_0\mathfrak{P}$, $s_1\mathfrak{P}$, $\cdots$, $s_{N-1}\mathfrak{P}$ all prime factors of p in $\mathfrak{K}$. Of these substitutions consider those which correspond to the substitutions of the complexes

$$gs_ig_z = gs_ig_zs_i^{-1}s_i \qquad (i=0, 1, \cdots, e-1).$$

Note that the group g_z leaves unchanged the ideal $\mathfrak{P}_0 = s_0\mathfrak{P} = \mathfrak{P}$, while the group $s_ig_zs_i^{-1}$ leaves unchanged $s_i\mathfrak{P} = \mathfrak{P}_i$ $(i=1, 2, \cdots, e-1)$, and the substitutions g of the realm $\mathfrak{k}$ leave unchanged the numbers of this realm and therefore the ideal $\mathfrak{p}$. It is then clear that $\frac{r \cdot r_z}{h_i}$ different substitutions of the complex gs_ig_z offer only one and the same prime ideal factor $\mathfrak{p}_i$ of p in $\mathfrak{k}$, and therefore it follows that there are only e different prime ideal factors

$$\mathfrak{p}_0, \mathfrak{p}_1, \cdots, \mathfrak{p}_{e-1} \tag{51}$$

of p in $\mathfrak{k}$.

Conforming to the above results, it is seen that $\mathfrak{p}_i$ is divisible by each of the prime ideal factors $s\mathfrak{P}$ of p, which correspond to the substitutions s of the complex gs_ig_z $(i=0, 1, \cdots, e-1)$, and we may add that $\mathfrak{p}_i$ *is divisible only by those ideals.*

To prove this, let $\mathfrak{P}'$ be a prime ideal divisor of p in $\mathfrak{K}$ different from the ideal divisor of p just mentioned, and let Ξ be a number of $\mathfrak{K}$ which is divisible by the product of the prime ideals $s\mathfrak{P}$ but otherwise is prime to p, so that

$$\Xi = \Pi s\mathfrak{P}\mathfrak{Q},$$

where the multiplication is to be taken over all the substitutions of the complex gs_ig_z, and where $\mathfrak{Q}$ is an ideal in $\mathfrak{K}$ that is relatively prime to p. That there exist

such numbers is seen in Arts. 20 and 87. Next let σ denote any substitution in g. It is seen that the application of σ to Ξ leaves the product $\Pi s\mathfrak{P}$ unchanged, while the conjugate ideal $\sigma\mathfrak{Q}$ remains prime to p. The product of the quantities $\sigma\Xi$, that is the relative norm of Ξ with respect to the realm $\mathfrak{k}$, is a quantity of $\mathfrak{k}$ which is divisible by the product $\Pi\sigma\mathfrak{P}$, and therefore it is divisible by the ideal $\mathfrak{P}_i$, and consequently also by $\mathfrak{p}_i$. On the other hand it is *not* contained in $\mathfrak{P}'$; accordingly $\mathfrak{p}_i$ is not divisible by $\mathfrak{P}'$.

To determine the *different* prime ideal factors of $\mathfrak{p}_i$, we must return to formula (49), in which $\bar{g}_i$ denotes the group of substitutions which are common to g and $g_z^{(i)} = s_i g_z s_i^{-1}$ and which therefore cause a change in neither $\mathfrak{p}_i$ nor $\mathfrak{P}_i$. We may write from (47)

$$gs_i g_z = gs_i g_z s_i^{-1} s_i = g g_z^{(i)} s_i = \sum_{k=1}^{k=e_i} s^{(k)} \bar{g}_i g_z^{(i)} s_i = \sum_{k=1}^{k=e_i} s^{(k)} g_z^{(i)} s_i;$$

and from this it is clear that there appear only e_i different prime ideals, namely the ideals

$$\mathfrak{P}_{i,k} = s^{(k)}\mathfrak{P}_i \qquad (k = 1, 2, \cdots, e_i),$$

which correspond to the prime ideal factor $\mathfrak{p}_i$ in $\mathfrak{k}$, these ideals being prime ideal factors of $\mathfrak{p}_i$ in $\mathfrak{K}$. We thus have the

$$e_0 + e_1 + \cdots + e_{e-1}$$

prime ideal factors, namely

$$(52)\quad \begin{cases} \mathfrak{P}_{0,1}, \quad \mathfrak{P}_{0,2}, \quad \cdots, \quad \mathfrak{P}_{0,e_0} \\ \qquad\qquad\qquad\qquad \text{prime ideal factors of } \mathfrak{p}_0, \\ \mathfrak{P}_{1,1}, \quad \mathfrak{P}_{1,2}, \quad \cdots, \quad \mathfrak{P}_{1,e_1} \\ \qquad\qquad\qquad\qquad \text{prime ideal factors of } \mathfrak{p}_1, \\ \cdots\quad\cdots\quad\cdots\quad\cdots \\ \cdots\quad\cdots\quad\cdots\quad\cdots \\ \cdots\quad\cdots\quad\cdots\quad\cdots \\ \mathfrak{P}_{e-1,1}, \quad \mathfrak{P}_{e-1,2}, \quad \cdots, \quad \mathfrak{P}_{e-1,e_{e-1}} \\ \qquad\qquad\qquad\qquad \text{prime ideal factors of } \mathfrak{p}_{e-1}; \end{cases}$$

and all the different prime ideal factors of p in $\mathfrak{R}$ must be found in the above scheme.

Next observe that each complex gs_ig_z contains $\frac{rr_z}{h_i}=r_ze_i$ different substitutions, while group G contains r_zn_z different substitutions. It follows that

$$r_z(e_0+e_1+\cdots+e_{e-1})=r_zn_z,$$

or

$$e_0+e_1+\cdots+e_{e-1}=n_z.$$

In other words, the *prime ideals (52) are the totality of all the different prime ideal factors of p in* $\mathfrak{R}$, *and consequently the e prime ideals* $\mathfrak{p}_0, \mathfrak{p}_1, \cdots, \mathfrak{p}_{e-1}$ *are in fact different from one another.*

To find the composition of these ideals out of those of (52), let $\mathfrak{P}_{i1}^{x_i}$ be the highest power of $\mathfrak{P}_{i1}$ that enters as a factor of $\mathfrak{p}_i$, so that we may write $\mathfrak{p}_i$, or more exactly $\mathfrak{O}\mathfrak{p}_i=\mathfrak{P}_{i1}^{x_i}\mathfrak{Q}$, where $\mathfrak{Q}$ is an ideal in $\mathfrak{R}$ that is not divisible by $\mathfrak{P}_{i1}$. Through application of the substitutions $s', s'', \cdots, s^{(e_i)}$ it is clear that $\mathfrak{O}\mathfrak{p}_i$ is also divisible by each of the ideals $\mathfrak{P}_{ik}$ $(k=2, \cdots, e_i)$, and consequently

$$\mathfrak{O}\mathfrak{p}_i=(\mathfrak{P}_{i1}\cdot\mathfrak{P}_{i2}\cdots\mathfrak{P}_{ie_i})^{x_i}, \tag{53}$$

where only the value of x_i remains to be determined. To determine this number observe that p, or more exactly $\mathfrak{O}p$, contains as a factor $\mathfrak{P}_{i1}=\mathfrak{P}_i$ to the power r_t [see formula (41)]; and this power of $\mathfrak{P}_i$ may be denoted by $\Pi s\mathfrak{P}_i$ where the product is to be taken over all those substitutions which do not change $\mathfrak{P}_i$ and that is over the group of substitutions $s_its_i^{-1}$, in which t goes over all the substitutions of the group g_t. Observe, however, that only those factors $s\mathfrak{P}_i$ of this product are divisors of $\mathfrak{p}_i$, where s is at the same time a substitution of $s_its_i^{-1}$ and g. Those substitutions that are common to the groups $s_ig_ts_i^{-1}=g_i^{(0)}$ and g form a group which we call $\bar{g}_i^{(0)}$. De-

note the degree of this group by t_i. Since $\bar{g}_i^{(0)}$ is a subgroup of g, t_i is a divisor of r_t, say

$$r_t = t_i d_i. \tag{54}$$

which determines d_i. Hence $\mathfrak{p}_i$ is divisible by t_i of the factors that constitute the product $\Pi s\mathfrak{P}$, the rest of these factors being divisors of ideals that are conjugates of $\mathfrak{p}_i$. Hence $\mathfrak{p}$ is divisible by $\mathfrak{P}_i$ exactly t_i times. Accordingly it is seen that $x_i = t_i$. It follows that

$$\mathfrak{O}\,\mathfrak{p}_i = (\mathfrak{P}_{i1} \cdot \mathfrak{P}_{i2} \cdots \mathfrak{P}_{ie_i})^{t_i}. \tag{55}$$

Further since p, or more exactly $\mathfrak{O}p$, contains the ideal factor $\mathfrak{P}_{i1}$ exactly r_t times, it follows that

$$\mathfrak{O}p = \mathfrak{p}_0^{d_0} \cdot \mathfrak{p}_1^{d_1} \cdots \mathfrak{p}_{e-1}^{d_{e-1}}. \tag{56}$$

It remains to determine the degrees of the ideal factors $\mathfrak{p}_0, \mathfrak{p}_1, \cdots \mathfrak{p}_{e-1}$. If f_i is the degree of $\mathfrak{p}_i$, we write

$$p^{f_i} = n(\mathfrak{p}_i), \tag{57}$$

where n denotes the norm of $\mathfrak{p}_i$ taken in the realm $\mathfrak{k}$, and that is, the product of the ideals conjugate to $\mathfrak{p}_i$. These are obtained, when one applies to $\mathfrak{p}_i$ the substitutions s of the group G which changes $\mathfrak{k}$ into its conjugate realms. Instead of these substitutions we apply all the substitutions of G. Then observe that each realm that is conjugate to $\mathfrak{p}_i$ appears r times, there being $\frac{N}{n} = r$ substitutions which do not change the numbers in $\mathfrak{k}$. Accordingly, we may write

$$p^{rf_i} = \Pi s\mathfrak{p}_i, \tag{58}$$

the product being taken over all the substitutions s of G. These substitutions, however, are also had through the complexes of substitutions (46), where in the complex gs_ig_z each substitution of the complex, as already shown, must be counted h_i times. Further observe that the substitutions s of this complex, and only these substi-

tutions, are the ones which determine the prime ideal $\mathfrak{p}_i$, so that there are in consequence $\frac{rr_z}{h_i} = e_i r_z$ substitutions of the complex $gg_z^{(t)}$, which are the substitutions of G for which $s\mathfrak{p}_i = \mathfrak{p}_i$. Hence among the factors $s\mathfrak{p}_i$ of the product (58) the prime ideal $\mathfrak{p}_i$ appears exactly $e_i r_z$ times. Since however, as seen from (56), the factor $\mathfrak{p}_i$ is found in the power p^{rf_i} exactly $rf_i d_i$ times, it is clear that

$$rf_i d_i = e_i r_z. \tag{59}$$

Since the group $g_i^{(t)} (= s_i g_t s_i^{-1})$ is a divisor of the group $g_z^{(t)} = s_i g_z s_i^{-1}$, observe that the group $\bar{g}_i^{(t)}$ of substitutions that are common to g and $s_i g_t s_i^{-1}$ is a divisor of $\bar{g}_i$, where $\bar{g}_i$ is constituted of the substitutions that are common to g and $s_i g_z s_i^{-1}$. Hence t_i, the number of substitutions of $\bar{g}_i^{(t)}$, is a divisor of h_i, the number of substitutions of $gs_i g_z$, so that we may write

$$h_i = t_i u_i, \tag{60}$$

where u_i is a rational integer and thus determined. It was seen further that there was a group $\bar{g}$ of degree h, whose substitutions were common to the two groups g and gsg_z and that $\frac{rr_z}{h}$ was equal to an integer. Similarly it is seen that in the complex $\bar{g}_i g_t^{(t)} = \bar{g}_i s_i g_t s_i^{-1}$ the number of substitutions that there are in common with g form a group $\bar{g}_t^{(t)}$ of degree t_i. Hence there are $\frac{r_t h_i}{t_i} = r_t u_i$ different substitutions, all of which are contained in the group $g_z^{(t)}$. For if s is a substitution of the group $\bar{g}_i$ belonging therefore to $g_z^{(t)}$ and consequently being of the form

$$s = s_i \sigma s_t^{-1}$$

where σ is a substitution of g_z, it follows that

$$\sigma^{-1} s_t^{-1} = s_t^{-1} s^{-1}.$$

We thus have

$$sg_i^{(1)}s^{-1} = ss_i \cdot g_i s_i^{-1}s^{-1} = s_i \sigma g_i \sigma^{-1} s_i^{-1};$$

or from formula (36)

$$sg_i^{(1)}s^{-1} = s_i g_i s_i^{-1} = g_i^{(1)}.$$

Hence for every substitution s of $\bar{g}_i$ and every substitution t in $g_i^{(1)}$ we can find a second substitution t_1 in $g_i^{(1)}$ such that $st = t_1 s$. If then s, s' are two substitutions of $\bar{g}_i$, while t, t' are two substitutions of $g_i^{(1)}$, then is

$$st \cdot s't' = s \cdot ts't' = s \cdot s't_1t' = s''t'',$$

where s'' belongs to $\bar{g}_i$ and t'' to $g_i^{(1)}$. Accordingly, the complex $\bar{g}_i g_i^{(1)}$ is in fact a group, and its degree $r_i u_i$ is a divisor of the degree of group $g_z^{(1)}$; that is

$$r_z = r_i u_i v_i, \tag{61}$$

where v_i is a rational integer and thus determined.

From (59) it was seen that $f_i d_i h = e_i r_z$; and from (50) and (61) this equality becomes $f_i d_i t_i = r_i v_i$, or due to (54)

$$f_i = v_i; \tag{62}$$

and this is the degree of the prime ideal $\mathfrak{p}_i$.

Finally denote by $\mathfrak{N}_i(\mathfrak{P}_{ik})$, the relative norm of the prime ideal $\mathfrak{P}_{ik}$ with respect to the realm $\mathfrak{k}$, and that is the product of the factors $s\mathfrak{P}_{ik}$ in which s goes over all substitutions of the group g. The formula (49) was

$$g = s'\bar{g}_i + s''\bar{g}_i + \cdots + s^{(e_i)}\bar{g}_i, \tag{49}$$

where s', s'', $\cdots$, $s^{(e_i)}$ are substitutions of g that do not belong to $\bar{g}_i$.

Again observe that the substitutions s of g fall into these e_i different complexes and that the substitutions of $\bar{g}_i$, being of the group $g_z^{(1)}$, leave unchanged the prime ideal $\mathfrak{P}_{ik}$. Consequently the operations of the substitutions s above bring into existence only the prime ideals $\mathfrak{P}_{i1}, \mathfrak{P}_{i2}, \cdots, \mathfrak{P}_{ie_i}$; and, since $r = h_i e_i$, each of these

ideals is repeated $h_i = t_i u_i$ times. Finally, due to formula (55), it is seen that

$$\mathfrak{N}_t(\mathfrak{P}_{ik}) = \mathfrak{p}_i^{u_i}. \tag{63}$$

The value of the exponent x_i in formula (53), namely in

$$\mathfrak{D}\mathfrak{p}_i = (\mathfrak{P}_{i1}\mathfrak{P}_{i2}\cdots\mathfrak{P}_{ie_i})^{x_i}$$

may also be determined in the following manner. Put for the prime ideal $\mathfrak{P}$ in Art. 242 the prime ideal $\mathfrak{P}_i = \mathfrak{P}_{i1}$, and let φ be the lowest power of z, such that

$$z^{\varphi} t = s,$$

where s is a substitution of the group g and t is a substitution of the inertia group.

From formula (32) it follows in general that

$$z^k \rho \equiv \rho^{p^k} \pmod{\mathfrak{P}_i};$$

and since $t\rho \equiv \rho \pmod{\mathfrak{P}_i}$, by definition of t, it is seen that

$$s\rho \equiv z^{\varphi} t\rho \equiv z^{\varphi}\rho \equiv \rho^{p^{\varphi}} \pmod{\mathfrak{P}_i},$$

and therefore, and more generally, for every integer Ω of the realm $\mathfrak{R}$ there exists the congruence

$$s\Omega \equiv \Omega^{p^{\varphi}} \pmod{\mathfrak{P}_i}.$$

Hence if ω is an integer of $\mathfrak{R}$, that is also an integer of $\mathfrak{k}$, it satisfies the congruence

$$\omega \equiv \omega^{p^{\varphi}} \pmod{\mathfrak{P}_i}.$$

However, since $\mathfrak{p}$ contains all integers of $\mathfrak{P}_i$ that are common to $\mathfrak{P}_i$ and $\mathfrak{k}$, it follows that

$$\omega \equiv \omega^{p^{\varphi}} \pmod{\mathfrak{p}_i}$$

for every integer ω of $\mathfrak{k}$. Hence φ is *not* less than f_i.

Since $\mathfrak{p}_i$ is divisible by $\mathfrak{P}_i$, and as ω is also an integer of $\mathfrak{R}$, it follows also that

$$\omega \equiv \omega^{p^{f_i}} \pmod{\mathfrak{P}_i}.$$

Further with respect to the realm $\mathfrak{k}$ of the rth degree, the integer ρ satisfies an equation of the rth degree, say

$$\rho^r + \omega'\rho^{r-1} + \omega''\rho^{r-2} + \cdots = 0, \tag{i}$$

where the coefficients ω', $\omega''\cdots$ are integers of $\mathfrak{k}$. Hence by raising (i) to the p^{f_i} power, it is seen that ρ also satisfies the congruence

$$\rho^{rp^{f_i}}+\omega'\rho^{(r-1)p^{f_i}}+\omega''\rho^{(r-2)p^{f_i}}+\cdots=0 \text{ (mod. } \mathfrak{P}_i).$$

Accordingly, it follows that $\rho^{p^{f_i}}$ is congruent (mod. $\mathfrak{P}_i$) to one of the roots of (i); and that is

$$\rho^{p^{f_i}}\equiv s\rho \text{ (mod. } \mathfrak{P}_i),$$

where s is a substitution of g. Due to the formula (32) it is seen that

$$z^{f_i}\rho\equiv s\rho \text{ (mod. } \mathfrak{P}_i),$$

and therefore more generally

$$z^{f_i}\Omega\equiv s\Omega \text{ (mod. } \mathfrak{P}_i)$$

for every integer Ω in $\mathfrak{R}$.

This congruence may be written in the form

$$z^{-f_i}s\rho\equiv\rho \text{ (mod. } \mathfrak{P}_i).$$

From this it is seen that $z^{-f_i}s$ belongs to the group g_t; and we may therefore write

$$z^{-f_i}s=t \qquad \text{or} \qquad z^{f_i}t=s;$$

and hence φ is not greater than f_i. It follows that

$$\varphi=f_i.$$

Since $\mathfrak{p}_i$ is divisible by $\mathfrak{P}_i$, we may write $\mathfrak{p}_i=\mathfrak{P}_i\mathfrak{Q}$; and taking the relative norm with respect to $\mathfrak{k}$, it is seen that

$$\mathfrak{p}_i^f=\mathfrak{N}_t(\mathfrak{P}_i)\cdot\mathfrak{N}_t(\mathfrak{Q}).$$

It follows that $\mathfrak{N}_t(\mathfrak{P}_i)$ is some power of $\mathfrak{p}_i$; say

$$\mathfrak{N}_t(\mathfrak{P}_i)=\mathfrak{p}_i^{\psi}.$$

On the other hand (see Art. 242)

$$p^f=N(\mathfrak{P}_i)=n\mathfrak{N}_t(\mathfrak{P}_i)=\mathfrak{N}_t n(\mathfrak{P}_i)=p^{f_i\psi}$$

so that

$$f=f_i\cdot\psi.$$

We saw that the degree of the group $\bar{g}_i$ of substitutions that are common to g and $g_z^{(1)}$ was divisible by the degree

of the group of substitutions that are common to g and $g_i^{(\mathfrak{f})}$, this group being $\bar{g}_i^{(\mathfrak{f})}$. From (34) it was seen that the substitutions of g_z could be distributed among the complexes $t, zt, z^2t, \cdots, z^{f-1}t$, in which t was a substitution of g_ι, where $z^f = t$ and where t in the different complexes went over the substitutions of g_ι. Similarly $\bar{g}_i$ may be distributed into the sum of the complexes

$$\bar{g}_i = \bar{g}_i^{(\mathfrak{f})} + z^{f_i}\bar{g}_i^{(\mathfrak{f})} + \cdots + z^{(\psi-1)f_i}\bar{g}_i^{(\mathfrak{f})},$$

where z is a substitution of g_z and satisfies, as proved above, the condition $z^{f_i}t = s$, where s belongs to $\bar{g}_i$ of degree h_i but not to $\bar{g}_i^{(\mathfrak{f})}$, while t is a substitution of $\bar{g}_i^{(\mathfrak{f})}$. It follows that $h_i = t_i\psi$. On the other hand from (60)

$$h_i = t_i u_i.$$

Hence it is seen that $\psi = u_i$.

In the derivation of formula (63), namely, $\mathfrak{N}_\iota(\mathfrak{P}_{ik}) = \mathfrak{p}_i^{u_i}$ it was seen that $\mathfrak{P}_{ik} = \mathfrak{P}_i$ occurs on the left hand member h_i times, whereas on the right hand side it occurs [see formula (53)] $x_i u_i$ times. Since $h_i = t_i u_i$, it follows that

$$t_i = x_i.$$

ART. **245.** The above results may be applied to certain special realms. For let $\mathfrak{k}$ be identical with the reduction realm, so that $g = g_z$ and sg_zs^{-1} become the groups of Art. 243. Since $g = g_z$, it follows [see (43) and (44)] that $r = r_z$ and therefore the group common to g_z and $sg_zs^{-1} = g_z$ is of degree $h = h_0 = r_z$.

From (61)

$$r_z = r_\iota u_i v_i = t_0 u_0 v_i$$

(from above)

$$= r_z v_i;$$

And consequently

$$v_i = v_0 = 1.$$

Since [see formula (54)] $r_\iota = d_0 t_0$ and $r_\iota = t_0$ (above), it follows that $d_0 = 1$.

Formula (55) takes the form

$$\mathfrak{O}\mathfrak{p}_0 = \mathfrak{P}_{01}^{r_t}, \tag{55'}$$

while (56) becomes

$$p = \mathfrak{p}_0 \mathfrak{q}, \tag{56'}$$

where $\mathfrak{q}$ is an ideal in $\mathfrak{k}$ that is not divisible by $\mathfrak{p}_0$. Since from (62) $f_i = v_i = 1$, it is seen from (57) that $n(\mathfrak{p}_0) = p$ and from (63) $\mathfrak{N}_{t_z}(\mathfrak{P}) = \mathfrak{p}_0'$.

Hence in the separation realm $\mathfrak{p}_0$ *is a prime ideal factor of* p *of the first degree which may be denoted by* $\mathfrak{p}_z$ *and in the Galois realm* $\mathfrak{p}_z$ *becomes the product of* r_t *equal factors* $\mathfrak{P}_{01} = \mathfrak{P}$, *each of degree* f. (See Hilbert, *Bericht*, p. 253.)

Next let $\mathfrak{k}$ be the inertia realm $\mathfrak{k}_t$, so that $g = g_t$ and $r = r_t$. The group $\bar{g}_0$ that contains the substitutions that are common to g and $s_0 g_z s_0^{-1} = g_z$ is identical with g_t. Its degree is $h_0 (= r_t)$, so that $e_0 = 1$. Further since the greatest common divisor of g and g_t is here g_t, its degree $t_0 = r_t$, $u_0 = 1$ and $v_0 = f$; and as $r_t = d_0 t_0$, we have finally $d_0 = 1$. Hence the general formula in this case becomes

$$p = \mathfrak{p}_0 \mathfrak{q}; \qquad \mathfrak{p}_0 = \mathfrak{P}^{r_t},$$
$$n(\mathfrak{p}_0) = p^f; \qquad \mathfrak{N}_{t_t}(\mathfrak{P}) = \mathfrak{p}_0.$$

And this shows, when we pass from the separation realm to the inertia realm, that the prime ideal $\mathfrak{p}_z$, which may be denoted by $\mathfrak{p}_t$ in the inertia realm, does not experience a separation into factors but is raised to a power, since the prime ideal which is of the first degree in the separation realm, is of the fth degree in the inertia realm.

Due to this fact, and observing that

$$(\mathfrak{O}_t, \mathfrak{p}_0) = n(\mathfrak{p}_0) = p^f,$$

and since

$$\mathfrak{p}_0 = \mathfrak{P}^{r_t},$$

it is seen that the integers of the inertia realm, and that is of $\mathfrak{O}_t$, are distributed (mod. $\mathfrak{P}^{r_t}$) into p^f classes of congruent integers. (See Theorem III, Art. 233.)

Observe that two numbers of a class (mod. $\mathfrak{P}^{r_t}$) belong to the same class (mod. $\mathfrak{P}$). Reciprocally, if two integers of the inertia realm are congruent (mod. $\mathfrak{P}$), their difference is an integer of the inertia realm as well as of the ideal $\mathfrak{P}$. Hence by the definition at the beginning of Art. 244, this difference is a number of the ideal $\mathfrak{p}_t = \mathfrak{p}_0$, and therefore is divisible by $\mathfrak{P}^{r_t}$. Hence the distribution of the integers of the inertia realm into classes (mod. $\mathfrak{P}^{r_t}$) is the same as it is, modulo $\mathfrak{P}$, so that the number of these classes is p^f (mod. $\mathfrak{P}$).

The numbers of the inertia realm all belong to the realm $\mathfrak{R}$ and the integers of $\mathfrak{R}$ [see formula (28)] may be distributed (mod. $\mathfrak{P}$) into p^f different classes.

Accordingly, every integer of the Galois realm is congruent (mod. $\mathfrak{P}$) to an integer of the inertia realm. (Hilbert, *Bericht*, p. 255.)

The inertia realm $\mathfrak{k}_t$ of degree $\frac{N}{r_t}$ is, with respect to the separation realm, of degree $\frac{N}{r_z}$ and hence it is a relative realm of degree

$$\frac{N}{r_t} \div \frac{N}{r_z} = \frac{r_z}{r_t} = f.$$

[See formula (35).] If then θ is an integer that generates the inertia realm, it must satisfy an irreducible equation in $\mathfrak{k}_z$ of the fth degree, say

$$\theta^f + \gamma_1 \theta^{f-1} + \cdots + \gamma_f = 0, \tag{64}$$

in which the coefficients are integers of $\mathfrak{k}_z$. Observe further that the substitutions

$$s_0(=1),\ z,\ z^2,\ \cdots,\ z^{f-1} \tag{65}$$

[see (34)] are substitutions of the reduction realm but not of the inertia realm, so that they change θ but not the γ's in (64).

The other roots of (64) are therefore had by applying these substitutions to θ.

If however, θ is a number of $\mathfrak{k}_t$, then $z\theta$ is also a number of the same realm. For as was seen above, corresponding to every substitution t of g_t there is another substitution t' of the same realm such that $tz = zt'$. Further for every number θ of $\mathfrak{k}$ the equation $t'\theta = \theta$ exists. Hence for every substitution t of g_t there exists the other relation

$$tz\theta = zt'\theta = z\theta,$$

so that $z\theta$ is a number of $\mathfrak{k}_t$ and as such is a rational function of θ.

Accordingly the equation (64) of the fth degree is, in the realm of rationality $\mathfrak{k}_z$, *a Galois equation with the group of substitutions (65) of degree f.*

ART. 246. The inertia realm in its turn is contained in a series of other sub-realms of $\mathfrak{K}$, of which each comprises the preceding. These sub-realms are such that upon transition of one to another the prime ideal $\mathfrak{p}_0 = \mathfrak{P}^{r_i}$ is continually reduced, until when the realm $\mathfrak{K}$ is reached this prime ideal becomes $\mathfrak{P}$. This was proved by Hilbert (see tables, *Bericht*, p. 258), the proof being as follows:

It has been seen that there exist in $\mathfrak{K}$ integers which are divisible by $\mathfrak{P}$ but not by $\mathfrak{P}^2$.

Among all the congruent (mod. $\mathfrak{P}$) integers of this kind there exists one (Art. 105), say π, that generates the realm $\mathfrak{K}$ so that $\mathfrak{K} = \mathfrak{R}(\pi)$. Further let ρ be a primitive number of $\mathfrak{K}$ (mod. $\mathfrak{P}$). Consequently all the integers of $\mathfrak{K}$ are congruent (mod. $\mathfrak{P}$) to one of the integers

$$0, 1, \rho, \rho^2, \cdots, \rho^{p^f-2}$$

(Vol. I, Art. 224), and it is further seen that

$$0, \pi, \pi\rho, \pi\rho^2, \cdots, \pi\rho^{p^f-2} \qquad \text{(i)}$$

constitute a system of p^f integers of $\mathfrak{P}$, which are

incongruent (mod. $\mathfrak{P}^2$). Also observe that

$$(\mathfrak{O}, \mathfrak{P}^2) = (\mathfrak{O}, \mathfrak{P})(\mathfrak{P}, \mathfrak{P}^2);$$

or

$$p^{2f} = p^f \cdot (\mathfrak{P}, \mathfrak{P}^2), \quad \text{so that} \quad (\mathfrak{P}, \mathfrak{P}^2) = p^f.$$

Thus there are p^f integers which present a complete system of residues of $\mathfrak{P}$ with respect to $\mathfrak{P}^2$, and every integer in $\mathfrak{P}$ is congruent (mod. $\mathfrak{P}^2$) to one of the integers in the series (i) above.

If t_i is a substitution of the inertia group, then by definition

$$t_i\Omega \equiv \Omega \pmod{\mathfrak{P}}$$

for every integer Ω of $\mathfrak{K}$; and in particular

$$t_i\pi \equiv \pi \pmod{\mathfrak{P}}.$$

Since

$$\pi \equiv 0 \pmod{\mathfrak{P}},$$

it follows that

$$t_i\pi \equiv 0 \pmod{\mathfrak{P}}.$$

In general, however,

$$t_i\pi \not\equiv 0 \pmod{\mathfrak{P}^2}.$$

On the other hand for every substitution t_i of the inertia group, there is one of the residues of (i) such that

$$t_i\pi \equiv \rho^{a_i}\pi \pmod{\mathfrak{P}^2}. \tag{66}$$

As there is an a_i corresponding to every t_i, let a be the smallest of these a_i and let t be the corresponding substitution so that

$$t\pi \equiv \rho^a\pi \pmod{\mathfrak{P}^2}. \tag{67}$$

If then in the sequel we denote by $(\mathfrak{P}^2)$ an integer that is contained in $\mathfrak{P}^2$, it is seen that (67) may be written in the form of an equation

$$t\pi = \rho^a\pi + (\mathfrak{P}^2).$$

It follows that

$$t^2\pi = (t\rho)^a t\pi + (\mathfrak{P}^2),$$

or

$$t^2\pi = [\rho^a + (\mathfrak{P})][\rho^a\pi + (\mathfrak{P}^2)] + (\mathfrak{P}^2),$$

which, when written as a congruence, is

$$t^2\pi \equiv \rho^{2a}\pi \pmod{\mathfrak{P}^2}.$$

And in general

(68) $$t^m\pi \equiv \rho^{ma}\pi \pmod{\mathfrak{P}^2}.$$

If k is the smallest positive integer for which $t^k = 1$, then $t^k\pi = \pi$; and $\rho^{ka}\pi \equiv \pi \pmod{\mathfrak{P}^2}$ or $\rho^{ka} \equiv 1 \pmod{\mathfrak{P}}$. It follows that

(69) $$t^{-m}\pi = t^{k-m}\pi \equiv \rho^{(k-m)a}\pi \equiv \rho^{-ma}\pi \pmod{\mathfrak{P}^2}.$$

Hence from (66) it is seen that

$$t^{-m}t_i\pi \equiv \rho^{+a_i}\rho^{-ma}\pi \equiv \rho^{a_i-ma}\pi \pmod{\mathfrak{P}^2},$$

where $t^{-m}t_i$ is a substitution of the inertia group. From this formula it is clear that, if a_i were not a multiple of a, we could so choose m that $a_i - ma$ is a positive integer less than a, and this is a contradiction to the definition of a.

From (68) it is seen that every multiple of a is found among the numbers a_i or is congruent to one of them (mod. $p^f - 1$). Hence, if h is the number of these different a_i's, they may all be denoted through

(70) $$0, a, 2a, \cdots, (h-1)a;$$

and it is further seen that ha must be equal to $p^f - 1$.

Accordingly h is a divisor of $p^f - 1$ and hence also h is relatively prime to p.

Next let v_i be those substitutions of the inertia group for which the exponent a_i in (66) is equal to zero, and that is,

(71) $$v_i\pi \equiv \pi \pmod{\mathfrak{P}^2}.$$

It is clear that these substitutions also have the character of a group and therefore form a sub-group of the inertia group, which Hilbert has called the *branch-group* (*Verzweigungsgruppe*) g_v of the prime ideal $\mathfrak{P}$. Its degree is a divisor of r_t, the degree of the inertia group, and may be denoted by r_v, while the corresponding realm, the

branch realm of $\mathfrak{P}$, is denoted by $\mathfrak{k}_v$ of degree $n_v > n_t$. (See Art. 234.)

Were the congruence (71) satisfied for all the substitutions of the inertia realm, that is if $h=1$, then would the branch-group g_v be identical with the inertia group. In this case $\mathfrak{k}_v$ and $\mathfrak{k}_t$ would be identical.

From (71) it follows that

$$v_i\pi - \pi = \mathfrak{P}^2\mathfrak{Q}, \tag{72}$$

where $\mathfrak{Q}$ is an ideal of $\mathfrak{K}$. Since $\pi^2 = \mathfrak{P}^2\mathfrak{A}$, where $\mathfrak{A}$ is an ideal of $\mathfrak{K}$ which is not divisible by $\mathfrak{P}$, it is seen that

$$\mathfrak{A}(v_i\pi - \pi) = \pi^2\mathfrak{Q},$$

and that is, for every integer α in $\mathfrak{A}$ there is an integer τ in $\mathfrak{Q}$ such that

$$\alpha(v_i\pi - \pi) = \pi^2\tau.$$

Hence if α is not divisible by $\mathfrak{P}$, and if $\alpha\gamma \equiv 1 \pmod{\mathfrak{P}}$ or $\alpha\gamma = 1 + (\mathfrak{P})$, it follows, if we put $\lambda = \tau\gamma$, that

$$v_i\pi = \pi + \pi^2\lambda \pmod{\mathfrak{P}^3}, \tag{i}$$

which in the form of an equation is

$$v_i\pi = \pi + \pi^2\lambda + (\mathfrak{P}^3).$$

Operating on this equation with the substitution v_i, it is seen that

$$v_i^2\pi = v_i\pi + v_i\pi^2 v_i\lambda + (\mathfrak{P}^3).$$

Observe that

$$v_i\pi^2 = (v_i\pi)^2 = \pi^2 + (\mathfrak{P}^3),$$

and by definition of v_i, that

$$v_i\lambda = \lambda + (\mathfrak{P}).$$

It follows that

$$v_i^2\pi = \pi + 2\pi^2\lambda \pmod{\mathfrak{P}^3}. \tag{ii}$$

Similarly it is seen that

$$v_i^3\pi = \pi + 3\pi^2\lambda \pmod{\mathfrak{P}^3}, \tag{iii}$$

. . . . . .

. . . . . .

and finally

$$v_i^p \pi \equiv \pi \pmod{\mathfrak{P}^3}.$$

In a similar manner

$$(73) \qquad \begin{cases} v_i^{p^2} \pi \equiv \pi \pmod{\mathfrak{P}^4}, \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ v_i^{p^{m-2}} \pi \equiv \pi \pmod{\mathfrak{P}^m}. \end{cases}$$

Observe that $v_i^{p^{m-2}}$ is a certain substitution of the branch-group. Since π is a quantity that determines the realm $\mathfrak{K} = \mathfrak{R}(\pi)$, it is clear that $v\pi - \pi$ is different from zero for all substitutions v except $v_0 = 1$. Suppose then that $\mathfrak{P}^\mu$ is the highest power of $\mathfrak{P}$ that is a divisor of $v\pi - \pi$ so that the congruence

$$v\pi \equiv \pi \pmod{\mathfrak{P}^{\mu+1}}$$

does *not* exist.

Writing $m = \mu + 1$ in (73), it follows that $v_i^{p^{\mu-1}} = s_0$, the identical substitution. Hence the smallest exponent k for which $v_i^k = s_0$ must be a divisor of $p^{\mu-1}$, that is, k must be a power of p. The same is true of r_v, the degree of the group, so that $r_v = p^l$, say, where l is a rational integer.

Due to formula (66) and what was proved in that connection, it is seen that for every substitution t_i there exists the congruence

$$t_i \pi \equiv \rho^{ma} \pi \pmod{\mathfrak{P}^2},$$

where m is one of the integers $0, 1, 2, \cdots, h-1$.

If t is the substitution that was used above, it is seen that

$$t^{-m} t_i \pi \equiv \pi \pmod{\mathfrak{P}^2},$$

or $t^{-m} t_i$ is a substitution of the branch group, say v. It follows that

$$(74) \qquad t^{-m} t_i = v, \qquad \text{or} \qquad t_i = t^m v.$$

Since all the substitutions of this form belong to the inertia group and are clearly different from one another,

we may write in the Galois sense

$$g_t = g_v + tg_v + t^2 g_v + \cdots + t^{h-1} g_v. \tag{75}$$

And that is: *the group g_t is composed of the complexes*

$$g_v,\ tg_v,\ t^2 g_v,\ \cdots,\ t^{h-1} g_v. \tag{76}$$

Accordingly, it is seen that

$$r_t = hr_v = hp^l. \tag{77}$$

Give to m the value found in formula (74) and observe by using (69) that

$$t_i t^{-m} \pi \equiv \pi \pmod{\mathfrak{P}^2}.$$

From this it follows that $t_i t^{-m} = v'$, where v' is a substitution of the branch-group; that is, $t_i = v' t^m$. From (74) it is seen that

$$v' t^m = t^m v \quad \text{or} \quad v' = t^m v t^{-m}, \tag{78}$$

a formula which *offers the invariance of the branch-group.*

Finally we may define the branch-group as *the collectivity of those substitutions v_i of the group G which satisfy the congruence*

$$v_i \Omega \equiv \Omega \pmod{\mathfrak{P}^2} \tag{79}$$

for every integer Ω of $\mathfrak{R}$. (Hilbert, *Bericht*, p. 255.) For it was seen in the preceding article that Ω of the realm $\mathfrak{R}$ is always congruent (mod. $\mathfrak{P}$) to some integer ω of $\mathfrak{k}_t$, or

$$\Omega - \omega \equiv 0 \pmod{\mathfrak{P}}.$$

It was also proved above that one or the other of the following congruences exists:

$1°,\ \Omega - \omega \equiv 0 \pmod{\mathfrak{P}^2}$ or $2°,\ \Omega - \omega \equiv \rho^\alpha \pi \pmod{\mathfrak{P}^2}$,

where α is one of the integers $0, 1, 2, \cdots, p^f - 2$. If v_i is a substitution of the branch-group, it belongs to the inertia group. When applied to ω, it leaves ω unchanged. Hence in case 2°, it is seen that

$$v_i \Omega - \omega \equiv v_i \rho^\alpha \cdot v_i \pi \pmod{\mathfrak{P}^2}.$$

Since $v_i\rho^\alpha = \rho^\alpha + (\mathfrak{P}^2)$ and $v_i\pi = \pi + (\mathfrak{P}^2)$ [see formula (71)], it follows that

$$v_i\rho^\alpha \cdot v_i\pi = \rho^\alpha\pi + (\mathfrak{P}^2).$$

We therefore have

$$v_i\Omega - \omega \equiv \rho^\alpha\pi \equiv \Omega - \omega \pmod{\mathfrak{P}^2},$$

a congruence which is also true in case 1°; that is

$$v_i\Omega \equiv \Omega \pmod{\mathfrak{P}^2}$$

for every integer Ω *of* $\mathfrak{K}$.

As π is an integer of $\mathfrak{K}$, it is seen that the congruence just written exists also for π and that is, v_i satisfies the congruence (71), through which the branch-group was defined. Since *a fortiori* the congruence

$$v_i\Omega \equiv \Omega \pmod{\mathfrak{P}}$$

exists for every integer Ω of $\mathfrak{K}$, it is clear that v_i is a substitution of the inertia group, being in particular a substitution of the branch-group.

If next we let $\mathfrak{k}_v$ denote the realm $\mathfrak{k}$ of Art. 243, so that

$$\mathfrak{k} = \mathfrak{k}_v, \qquad g = g_v, \qquad r = r_v = p^l,$$

then $\bar{g}_0$, the group common to g_v and g_z, is here g_v, so that $h_0 = r_v$ and $e_0 = 1$.

Further the substitutions common to g and g_t form here the group g_v, so that $t_0 = r_v$, $u_0 = 1$, $v_0 = f$ [see formulas (50), (62) and (40)]. Due to formula (77), since $r_t = d_0 t_0$ [formula (54)], it is seen that $d_0 = h$.

It follows that the general formulas of Art. 244 take here the form

$$\mathfrak{D}\mathfrak{p}_0 = \mathfrak{P}^{r_v}, \qquad n(\mathfrak{p}_0) = p^f;$$

and it is seen that $\mathfrak{p}_v = \mathfrak{P}^{r_v}$ *is a prime ideal factor of* p *of degree* f *in the branch realm, and consequently the prime ideal* $\mathfrak{p}_z = \mathfrak{p}_t = \mathfrak{p}^{r_t}$ *by transition to the branch realm, which contains the inertia realm (due to the relation* $\mathfrak{p}_z = \mathfrak{p}_t = \mathfrak{p}_v^h$*) is factorable into* h *equal prime ideal factors of the* f*th degree.*

(Hilbert, p. 256.)

The branch realm $\mathfrak{k}_v$ of degree $\frac{N}{r_v}=n_v$ is, with regard to the inertia realm, which is of degree $n_\iota=\frac{N}{r_\iota}$, a relative realm of degree

$$\frac{n_v}{n_\iota}=\frac{r_\iota}{r_v}=h.$$

Hence an integer η which produces the realm $\mathfrak{k}_v$ satisfies in $\mathfrak{k}_\iota$ an irreducible equation of the hth degree:

$$\eta^h+\delta_1\eta^{h-1}+\delta_2\eta^{h-2}+\cdots+\delta_h=0, \tag{80}$$

where the δ's are integers in $\mathfrak{k}_\iota$.

And the other roots are had through application of the substitutions of the inertia group which do not belong to the branch-group, and that is through the substitutions

$$t_0=s_0(=1),\ t,\ t^2,\ \cdots,\ t^{h-1}, \tag{81}$$

where t is the substitution employed in (76). If, however, η is any number of $\mathfrak{k}_v$, then also are $t^m\eta$ ($m=1, 2, \cdots, h-1$) numbers of $\mathfrak{k}_v$. For, due to formula (78), corresponding to every substitution v' of the branch-group there exists a substitution of the same group, for which $t^mv=v't^m$. Further since $v\eta=\eta$ for every integer η of $\mathfrak{k}_v$, it follows that

$$v't^m\eta=t^mv\eta=t^m\eta,$$

so that the number $t^m\eta$ is a number of $\mathfrak{k}_v$; and since η may be taken as an integer which produces $\mathfrak{k}_v$, it follows also that $t^m\eta$ is a rational function of η and accordingly the equation (80) is, with respect to $\mathfrak{k}_v$, *a relative Galois equation with the cyclic group of substitutions (81) of degree h.*

ART. **247.** Since the congruence (71) exists for every substitution of the branch-group g_v, it may be possible

that this congruence exists for a power of $\mathfrak{P}$ higher than 2 as the modulus.

Suppose then that the congruence

$$v_i\pi \equiv \pi \pmod{\mathfrak{P}^\lambda} \qquad (\lambda \geqq 2) \tag{82}$$

exists for every substitution v_i of g_v, it being presupposed, however, that the congruence

$$v_i\pi \equiv \pi \pmod{\mathfrak{P}^{\lambda+1}}$$

does *not* exist for every such substitution.

It is clear that those substitutions $\bar{v}_i$ of g_v, for which

$$\bar{v}_i\pi \equiv \pi \pmod{\mathfrak{P}^{\lambda+1}},$$

form a new group, a sub-group of g_v. This group may be called a *one-stroked branch-group* $g_{\bar{v}}$ of the prime ideal $\mathfrak{P}$. The associated realm is called the *one-stroked branch realm* of the prime ideal $\mathfrak{P}$. Its degree may be denoted by $n_{\bar{v}}$ while $r_{\bar{v}}$ denotes the degree of $g_{\bar{v}}$. Since the latter is a divisor of $r_v = p^l$, it must be a power of p say $p^{\bar{l}}$. Writing $l - \bar{l} = \bar{e}$, it is seen that

$$r_v = r_{\bar{v}} p^{\bar{e}}. \tag{84}$$

Accordingly, the group g_v consists of $p^{\bar{e}}$ complexes of the form

$$v_0 g_{\bar{v}} = g_{\bar{v}},\ v_1 g_{\bar{v}},\ v_2 g_{\bar{v}},\ \cdots,\ v_{p^{\bar{e}}-1} g_{\bar{v}}; \tag{85}$$

and it shall be proved that the substitutions

$$v_0 = s_0,\ v_1,\ v_2,\ \cdots,\ v_{p^{\bar{e}}-1} \tag{86}$$

which, excepting v_0, do not belong to $g_{\bar{v}}$, have the property that for any arbitrary two, say v_i and v_k, the relation

$$v_i v_k = v_k v_i \bar{v} \tag{87}$$

exists, where $\bar{v}$ is a substitution of $g_{\bar{v}}$.

It was proved (see Art. 64) that every integer Ω of $\mathfrak{R}$ was congruent (mod. $\mathfrak{P}^{\lambda+1}$) to an expression

$$\alpha_0 + \alpha_1\pi + \alpha_2\pi^2 + \cdots + \alpha_\lambda\pi^\lambda,$$

where the coefficients α_i are integers in $\mathfrak{K}$. More particularly, we may assume that these coefficients are integers of the inertia realm. For it was proved in Art. 245 that any integer of $\mathfrak{K}$ was congruent (mod. $\mathfrak{P}$) to an integer α_0 of $\mathfrak{k}_t$; and that is $\Omega = \alpha_0 + \mathfrak{P}\mathfrak{Q}$, where $\mathfrak{Q}$ is an ideal of $\mathfrak{K}$. Since $\pi = \mathfrak{P}\mathfrak{A}$, $\mathfrak{A}$ being an ideal in $\mathfrak{K}$, it follows that

$$\mathfrak{A}(\Omega - \alpha_0) = \pi\mathfrak{Q} \qquad \text{or} \qquad \alpha(\Omega - \alpha_0) = \pi\tau,$$

where α and τ are integers of $\mathfrak{A}$ and $\mathfrak{Q}$ respectively and α is *not* divisible by $\mathfrak{P}$. Hence if $\alpha\gamma \equiv 1$ (mod. $\mathfrak{P}$), or $\alpha\gamma = 1 + (\mathfrak{P})$, it is seen that $\Omega - \alpha_0 = \pi\sigma$ (mod. $\mathfrak{P}^2$), where $\sigma = \gamma\tau$ is an integer in $\mathfrak{K}$, which may be taken (mod. $\mathfrak{P}$) congruent to α_1, α_1 being an integer in $\mathfrak{k}_t$. It follows that

$$\Omega \equiv \alpha_0 + \alpha_1\pi \text{ (mod. } \mathfrak{P}^2);$$

and by repetition of this process, it is seen that

$$\Omega \equiv \alpha_0 + \alpha_1\pi + \alpha_2\pi^2 + \cdots + \alpha_\lambda\pi^\lambda \text{ (mod. } \mathfrak{P}^{\lambda+1}),$$

where the α's are integers of $\mathfrak{k}_t$.

From formula (82) it is seen that $v_i\pi = \pi + \mathfrak{P}^\lambda\mathfrak{Q}$, where $\mathfrak{Q}$ is an ideal in $\mathfrak{K}$.

If

$$\pi^\lambda = \mathfrak{P}^\lambda\mathfrak{A},$$

then is

$$\mathfrak{A}(v_i\pi - \pi) = \pi^\lambda\mathfrak{Q};$$

and as above

(88) $$v_i\pi \equiv \pi + \pi^\lambda\sigma_i$$

and similarly,

$$v_k\pi \equiv \pi + \pi^\lambda\sigma_k \text{ (mod. } \mathfrak{P}^{\lambda+1}),$$

where σ_i and σ_k are integers in $\mathfrak{K}$.

Accordingly, it is seen that

$$v_k\pi^\lambda = \pi^\lambda + (\mathfrak{P}^{\lambda+1}),$$

while

$$v_k\sigma_i = \sigma_i + (\mathfrak{P}),$$

and consequently

$$v_k(\sigma_i\pi^\lambda) = \sigma_i\pi^\lambda + (\mathfrak{P}^{\lambda+1}).$$

Hence from (88) it is seen that

$$v_k v_i \pi \equiv v_k \pi + v_k(\pi^\lambda \sigma_i) \text{ (mod. } \mathfrak{P}^{\lambda+1})$$
$$\equiv \pi + \pi^\lambda \sigma_k + \pi^\lambda \sigma_i \text{ (mod. } \mathfrak{P}^{\lambda+1});$$

and similarly

$$v_i v_k \pi \equiv \pi + \pi^\lambda \sigma_i + \pi^\lambda \sigma_k \text{ (mod. } \mathfrak{P}^{\lambda+1}),$$

so that finally

$$v_k v_i \pi \equiv v_i v_k \pi \text{ (mod. } \mathfrak{P}^{\lambda+1}).$$

If then, as above, any integer Ω of $\mathfrak{K}$ is expressed through a congruence (mod. $\mathfrak{P}^{\lambda+1}$) in a power series of π, and if we observe that the coefficients α of this power series (being integers of $\mathfrak{k}$) remain unchanged when operated upon by the substitutions v_i, v_k of the group g_ι, it is clear that

$$v_k v_i \Omega \equiv v_i v_k \Omega \text{ (mod. } \mathfrak{P}^{\lambda+1}),$$

or

$$v_k^{-1} v_i^{-1} v_k v_i \Omega \equiv \Omega \text{ (mod. } \mathfrak{P}^{\lambda+1}).$$

It follows that the substitution $v_k^{-1} v_i^{-1} v_k v_i$ is a substitution, $\bar{v}$ say, of the one-stroked branch-group $g_{\bar{v}}$. And from this it is seen that

$$v_k v_i = v_i v_k \bar{v},$$

where v_k, v_i are arbitrary substitutions of g_v. If in particular v_k is a substitution $\bar{v}'$ of $g_{\bar{v}}$, then is $\bar{v}' v_i = v_i \bar{v}''$, where $\bar{v}''$ is a substitution of $g_{\bar{v}}$.

Next take the one-stroked branch realm $\mathfrak{k}_{\bar{v}}$ in place of the sub-realm $\mathfrak{k}$ of Art. 243. If $\mathfrak{k} = \mathfrak{k}_{\bar{v}}$, it follows that

$$g = g_{\bar{v}}, \qquad r = r_{\bar{v}} = p^{\bar{\iota}},$$

while g_0, the group common to g and g_z, becomes identical with $g_{\bar{v}}$, so that $h_0 = r_{\bar{v}}$, $e_0 = 1$, and $t_0 = r_{\bar{v}}$, $u_0 = 1$, $v_0 = f$.

Further, since $r_\iota = d_0 t_0 = d_0 r_{\bar{v}}$ and $r_\iota = h r_v$, while $r_v = p^\iota$, it follows that $d_0 = h p^{\iota - \bar{\iota}}$, or $d_0 = h p^{\bar{e}}$. Accordingly, observe that in Art. 244 the prime ideal $\mathfrak{p}_0$ becomes here the ideal $\mathfrak{p}_{\bar{v}}$ of the realm $\mathfrak{k}_{\bar{v}}$, the general formulas being

$$\mathfrak{p}_{\bar{\mathfrak{p}}} = \mathfrak{P}^{r_{\bar{v}}} = \mathfrak{P}^{p^{\bar{\iota}}}, \qquad \text{while} \qquad n(\mathfrak{p}_{\bar{v}}) = p^f.$$

Note that the prime ideal $\mathfrak{p}_v = \mathfrak{P}^{r_v}$ is of the fth degree in the branch realm $\mathfrak{k}_v$, and that when a transition is made to the one-stroked realm $\mathfrak{k}_{\bar{v}}$, which contains $\mathfrak{k}_v$ it is seen, due to formula

$$(\mathfrak{p}_{\bar{v}})^{p^{\bar{e}}} = \mathfrak{P}^{p^{\bar{e}}.\, p^{e-\bar{e}}} = \mathfrak{P}^{p^e},$$

that $\mathfrak{p}_v$ becomes factorable into $p^{\bar{e}}$ prime factors, each of degree f. The realm $\mathfrak{k}_{\bar{v}}$ is, with respect to $\mathfrak{k}_v$, a realm of degree

$$\frac{n_{\bar{v}}}{n_v} = \frac{r_v}{r_{\bar{v}}} = p^{\bar{e}}.$$

And if $\bar{\eta}$ is an integer which produces this realm, then $\bar{\eta}$ satisfies in the realm $\mathfrak{k}_v$ an irreducible equation of the $p^{\bar{e}}$ degree of the form

$$\bar{\eta}^{p^{\bar{e}}} + \bar{\delta}_1 \bar{\eta}^{p^{\bar{e}}-1} + \cdots + \bar{\delta}_{p^{\bar{e}}} = 0, \tag{90}$$

where the $\bar{\delta}$'s are integers in $\mathfrak{k}_v$. This equation, relative to $\mathfrak{k}_v$, is an *Abelian equation*. For the other roots of (90) that are conjugate to $\bar{\eta}$ are had, if $\bar{\eta}$ is subjected to the substitutions g_v which do not belong to $g_{\bar{v}}$, and that is, to the substitutions (86). If v_i is any of these substitutions, then due to formula (89) corresponding to every substitution $\bar{v}'$ of g_v another substitution $\bar{v}''$ of g_v may always be determined, such that

$$\bar{v}' v_i \bar{\eta} = v_i \bar{v}'' \bar{\eta} = v_i \bar{\eta}.$$

And that is, the integer $v_i\bar{\eta}$ remains unaltered, when subjected to the substitutions of $g_{\bar{v}}$, and consequently $v_i\bar{\eta}$ belongs to the realm $\mathfrak{k}_{\bar{v}}$. This proves that every root of (90) may be expressed rationally through $\bar{\eta}$ and the numbers of the realm $\mathfrak{k}_v$.

Accordingly, write

$$v_i\bar{\eta} = f_i(\bar{\eta});$$

and similarly, if v_k is any of the other substitutions (86), put

$$v_k\bar{\eta} = f_k(\bar{\eta}).$$

It follows that

$$v_k v_i \bar{\eta} = f_i f_k(\bar{\eta}) \qquad \text{and} \qquad v_i v_k \bar{\eta} = f_k f_i(\bar{\eta}).$$

Further if $\bar{v}$ is a substitution determined as in (87), so that

$$v_i v_k = v_k v_i \bar{v}, \qquad \text{then is} \qquad v_i v_k \bar{\eta} = v_k v_i \bar{v}\bar{\eta} = v_k v_i \bar{\eta}.$$

And that is

$$f_k f_i(\bar{\eta}) = f_i f_k(\bar{\eta}).$$

This proves that the equation (90), relative to $\mathfrak{k}_v$, is an Abelian equation.

ART. 248. We may continue in a similar manner. Let λ denote the highest exponent such that for all substitutions $\bar{v}$ of $g_{\bar{v}}$ the congruence

$$\bar{v}\pi \equiv \pi \pmod{\mathfrak{p}^{\lambda}}$$

is satisfied, while the congruence

$$\bar{v}\pi \equiv \pi \pmod{\mathfrak{p}^{\lambda+1}}$$

is *not* satisfied for all the substitutions $\bar{v}$ of $g_{\bar{v}}$. Then those substitutions of g_v which do satisfy the latter congruence, constitute a new group, a *two-stroked branch-group*, $g_{\bar{\bar{v}}}$ of $\mathfrak{P}$, and this group is contained in $g_{\bar{v}}$. Its associated realm may be called the two-stroked branch realm.

It is clear that this new group $g_{\bar{\bar{v}}}$ is related to $g_{\bar{\bar{v}}}$ in precisely the same way that $g_{\bar{v}}$ is to g_v. The analogous results may be worded as follows: *The degree of $g_{\bar{\bar{v}}}$ is a power of p, say $p^{\bar{\bar{l}}}$, and if we put $\bar{l} - \bar{\bar{l}} = \bar{\bar{e}}$, the prime ideal $\mathfrak{p}_{\bar{v}}$ upon transition from the one-stroked to the two-stroked branch-group, due to the formula*

$$\mathfrak{p}_{\bar{\bar{v}}} = (\mathfrak{p}_{\bar{\bar{v}}})^{p^{\bar{\bar{e}}}}$$

is factorable into $p^{\bar{\bar{l}}}$ equal prime ideal factors of the fth degree that belong to the realm $\mathfrak{k}_{\bar{\bar{v}}}$; and, moreover, the integer $\bar{\bar{\eta}}$, which produces $\mathfrak{k}_{\bar{\bar{v}}}$, satisfies an irreducible equation of the $p^{\bar{\bar{e}}}$ degree, which with respect to $\mathfrak{k}_{\bar{v}}$, is an Abelian equation.

In the same way if we proceed to a three- or more-stroked branch realm, it is clear that there is further factorization of the prime ideal factors of p. Since each of these successive realms is a super-realm of the one immediately preceding, its degree is also a multiple of the degree of the preceding one; and finally one of these realms must be identical with $\mathfrak{R}$ itself. With this the process is closed and the ideal $\mathfrak{P}$ itself appears as the ideal factor of p. The results that have been derived are found in the following table, in which the realm $\mathfrak{R}$ is assumed to be a three-stroked realm. (Hilbert, *Bericht*, p. 258.)

$\mathfrak{k}_z$	$\mathfrak{k}_t$	$\mathfrak{k}_v$	$\mathfrak{k}_{\bar{v}}$	$\mathfrak{k}_{\bar{\bar{v}}}$	$\mathfrak{R}$
r_z	r_t	r_v	$r_{\bar{v}}$	$r_{\bar{\bar{v}}}$	1
$n_z=\frac{N}{r_z}$	$n_t=\frac{N}{r_t}$	$n_v=\frac{N}{r_v}$	$n_{\bar{v}}=\frac{N}{r_{\bar{v}}}$	$n_{\bar{\bar{v}}}=\frac{N}{r_{\bar{\bar{v}}}}$	N
	$f=\frac{r_z}{r_t}$	$h=\frac{r_t}{r_v}$	$p^{\bar{e}}=\frac{r_v}{r_{\bar{v}}}$	$p^{\bar{\bar{e}}}=\frac{r_{\bar{v}}}{r_{\bar{\bar{v}}}}$	$p^{\bar{\bar{e}}}=r_{\bar{\bar{v}}}$
$\mathfrak{p}=\mathfrak{p}_v^h=\mathfrak{P}^{r_t}$		$\mathfrak{p}_v=\mathfrak{p}_{\bar{v}}^{p^{\bar{e}}}$ $=\mathfrak{P}^{r_{\bar{v}}}$	$\mathfrak{p}_{\bar{v}}=\mathfrak{p}_{\bar{\bar{v}}}^{p^{\bar{\bar{e}}}}$ $=\mathfrak{P}^{r_{\bar{v}}}$	$\mathfrak{p}_{\bar{\bar{v}}}=\mathfrak{P}^{p^{\bar{\bar{e}}}}$ $=\mathfrak{P}^{r_{\bar{\bar{v}}}}$	$\mathfrak{P}$

In the first row are found the realms that have been considered; in the second row are given the degrees of the corresponding groups; in the third row we have the degrees of the realms; in the fourth are the relative degrees with respect to the next lowest realm; and finally in the last row appear the prime ideals of the realms and their values in terms of powers of $\mathfrak{P}$.

The fact that the degree N of the group G is a multiple of the degree of each of its sub-groups, while the degrees of the branch-groups are powers of p, shows that, if N is not divisible by p, there can be no stroked branch-groups or realms present, and that a branch-group $\mathfrak{k}_v$ can only

exist if $r_v = p^l = 1$, and that is, only if the group g_v consists of the identical substitution. In this case the branch realm $\mathfrak{k}_v$ is identical with $\mathfrak{K}$.

More generally, this identity will exist also in the case where N *is* divisible by p, while the degree r_t of the inertia group is *not* divisible by p. For due to the fact that $r_t = hr_v = hp^l$, it follows that $p^l = 1$.

If, however, r_t is divisible by p, this same relation shows, since h is not divisible by p, that $r_v = p^l > 1$; and in this case $\mathfrak{k}_v$ is a sub-realm different from $\mathfrak{K}$, so that there is at least a one-stroked branch realm present.

It is further seen from the theorems relative to the equations through which are determined the integers that produce the series of realms, that the integer A, which generates the Galois realm $\mathfrak{K}$, satisfies, with respect to the nearest sub-realm of the series, an Abelian equation; or, if $\mathfrak{K}$ is identical with the branch realm or the inertia realm, then the integer A satisfies a cyclic equation with respect to $\mathfrak{k}_t$, or with respect to $\mathfrak{k}_z$ respectively. In other words: The inertia realm $\mathfrak{k}_t$ is relative-cyclic with the relative-degree f with respect to the separation realm $\mathfrak{k}_z$; the branch realm $\mathfrak{k}_v$ is relative-cyclic of degree h with respect to the inertia realm $\mathfrak{k}_t$. The one-stroked branch realm $\mathfrak{k}_{\bar{v}}$ is a relative Abelian realm of relative degree $p^{\bar{e}}$ with respect to $\mathfrak{k}_v$; the realm $\mathfrak{k}_{\bar{\bar{v}}}$ is a relative Abelian realm of relative degree $p^{\bar{\bar{e}}}$ with respect to $\mathfrak{k}_{\bar{v}}$. Observe that the degree of each Abelian equation is a power of p and that A is expressed through the integer that produces the first preceding sub-realm by the extraction of roots. The integer, however, that produces this sub-realm in turn is expressed through those which generate the next sub-realm, so that finally the integer A that generates $\mathfrak{K} = \mathfrak{R}(A)$, that is the Galois realm, is determined through the integer that produces

the separation realm by means of extraction of roots. And this result of Hilbert may be expressed as follows:

The separation realm of every prime ideal in the Galois realm is a realm of rationality, in which the numbers of the Galois realm are to be had through expressions which involve only the extraction of roots. (Hilbert, *Bericht*, p. 263.)

This theorem offers, besides its importance relative to the algebraic solution of equations, another highly interesting feature in that the intimate relation between the theory of numbers and algebra is brought to light in a pleasing manner.

The theorem shows that it is just those realms which are used in the gradual factorization of p into its prime ideal factors that are also adapted to offering the algebraic solution of the equation through which the Galois realm is determined.

The Hilbert theorem puts in a clear light the significance of the theory of those algebraic equations that admit solution through the extraction of roots.

ART. **249.** We are now in a position, through the consideration of the above series of sub-realms of the Galois realm, to determine the exact power of $\mathfrak{P}$, as well as of p, which is a divisor of the different or of the discriminant of the Galois realm. To this end the following theorems must be proved:

THEOREM I. *The different of the inertia realm is not divisible by the prime ideal* $\mathfrak{P}$.

If $\omega_1, \omega_2, \cdots$, form a basis of all integers in $\mathfrak{k}_t$, the elements of $\mathfrak{k}_t$ are ideals in $\mathfrak{K}$, namely,

$$\mathfrak{e}' = \{\omega_1 - s\omega_1,\ \omega_2 - s\omega_2,\ \omega_3 - s\omega_3,\ \cdots\},\ \text{etc.},$$

where s is a substitution of $\mathfrak{K}$, that does not belong to the inertia group. Observe that the different (Art. 77) is the product of these elements. Now one of these

elements can be divisible by $\mathfrak{P}$ only if each of the differences $\omega_i - s\omega_i$ is divisible by $\mathfrak{P}$ and therefore also if for every integer ω of $\mathfrak{k}_t$ the difference $\omega - s\omega$ is divisible by $\mathfrak{P}$.

If then ω is any integer of the prime ideal $\mathfrak{p}_t (= \mathfrak{P}^{r_t})$ of $\mathfrak{k}_t$, then is ω divisible by $\mathfrak{P}$, and as $\omega - s\omega$ is divisible by $\mathfrak{P}$, it follows also that $s\omega$ is divisible by $\mathfrak{P}$, and therefore also $s\mathfrak{p}_t = (s\mathfrak{P})^{r_t}$ is divisible by the prime ideal $\mathfrak{P}$ and consequently $s\mathfrak{P} = \mathfrak{P}$.

In Art. 245 it was seen that every integer Ω in $\mathfrak{K}$ was congruent (mod. $\mathfrak{P}$) to some integer ω in $\mathfrak{k}_t$; and that is

$$\Omega \equiv \omega \pmod{\mathfrak{P}}.$$

It also follows that

$$s\Omega \equiv s\omega \pmod{s\mathfrak{P}},$$

or

$$s\Omega \equiv s\omega \pmod{\mathfrak{P}}.$$

It follows, if $s\omega \equiv \omega$, that

$$s\Omega \equiv \Omega \pmod{\mathfrak{P}}.$$

Accordingly, s belongs to the substitutions of the inertia group, contrary to the hypothesis made regarding this substitution.

THEOREM II. *The relative different of the branch realm $\mathfrak{k}_v$ relative to the inertia realm $\mathfrak{k}_t$ is divisible by $\mathfrak{P}^{r_t - r_v} = \mathfrak{p}^{h-1}$, but by no higher power of $\mathfrak{P}$.* (Hilbert, *Bericht*, p. 259.)

For this case let $\omega_1, \omega_2, \omega_3, \cdots$ be a basis of all integers of $\mathfrak{k}_v$. Then is every element of $\mathfrak{k}_v$ that enters as a factor of the relative different an ideal of the Galois realm, namely

$$(91) \qquad (\omega_1 - \tau\omega_1,\ \omega_2 - \tau\omega_2,\ \omega_3 - \tau\omega_3,\ \cdots),$$

where τ goes over each of the substitutions t^m ($m = 1, 2, \cdots, h-1$) of the group g_t, which is not *a* a substitution of g_v. [See formula (76).]

Observe that for every integer Ω of $\mathfrak{K}$, therefore *a fortiori* for every integer ω of $\mathfrak{k}_v$, the difference $\omega - \tau\omega$ is divisible by $\mathfrak{P}$. This difference is also a number of $\mathfrak{k}_v$,

owing to the fact that for every substitution v of the branch-group there exists another substitution v' of the same group, such that

$$t^m v' = v t^m,$$

and therefore

$$v(\omega - t^m\omega) = v\omega - t^m v'\omega = (\omega - t^m\omega).$$

From this it is seen that $\omega - t^m\omega$ is unchanged by every substitution of g_v.

Accordingly, $\omega - t^m\omega$ is a number of the ideal $\mathfrak{p}_v (= \mathfrak{P}^{r_v})$, which, by definition, consists of all numbers common to $\mathfrak{P}$ and $\mathfrak{k}_v$. It follows that $\omega - t^m\omega$ is divisible by $\mathfrak{P}^{r_v}$.

It is thus seen that each of the elements (91) is divisible by $\mathfrak{P}^{r_v}$, and these elements are all ideals of $\mathfrak{P}$. It will be proved next that none of these ideals (91) is divisible by a higher power of $\mathfrak{P}$. For were there a higher power of $\mathfrak{P}$ as factor, it would follow that each of the differences $\omega_i - t^m\omega_i$, and therefore also for every integer ω of $\mathfrak{k}_v$ the difference $\omega - t^m\omega$ would be divisible by $\mathfrak{P}^{r_v+1}$. It may be proved, however, that there is a number of $\mathfrak{k}_v$ for which this is not true.

For (Art. 63) let ω be a number in $\mathfrak{k}_v$ that is divisible by $\mathfrak{p}_v (= \mathfrak{P}^{r_v})$ but which is not divisible by $\mathfrak{p}_v^2$, and let π be an integer of $\mathfrak{K}$ (Art. 245) that is divisible by $\mathfrak{P}$ but not by $\mathfrak{P}^2$. Let π be a primitive integer of $\mathfrak{K}$ (mod. $\mathfrak{P}$). We may then write

$$\omega = \mathfrak{P}^{r_v}\mathfrak{Q}, \qquad \pi = \mathfrak{P}\mathfrak{A},$$

where $\mathfrak{Q}$ and $\mathfrak{A}$ are ideals of $\mathfrak{K}$, which are not divisible by $\mathfrak{P}$. It follows that

$$\mathfrak{A}^{r_v}\omega = \pi^{r_v}\mathfrak{Q}.$$

Accordingly, there is an integer α of $\mathfrak{A}^{r_v}$ that is not divisible by $\mathfrak{P}$ and a corresponding integer τ of $\mathfrak{Q}$, such that

$$\alpha\omega = \pi^{r_v}\tau.$$

If further

$$\alpha\gamma \equiv 1 \pmod{\mathfrak{P}},$$

it is seen that

$$\omega \equiv \pi^{r_v}\sigma \pmod{\mathfrak{P}^{r_v+1}}, \qquad \text{where} \qquad \tau\gamma = \sigma.$$

It also follows that

$$\omega \equiv \pi^{r_v}\rho^{\mu} \pmod{\mathfrak{P}^{r_v+1}}, \tag{92}$$

where μ is [see formula (66)] one of the numbers 0, 1, $2, \cdots, p, \cdots, p^f-2$.

For each of the substitutions t^m which belong to g_t but not to g_v we may write [see formula (67)]

$$t^m\pi \equiv \rho^{\alpha}\pi \pmod{\mathfrak{P}^2},$$

where α is one of the numbers

$$a, 2a, 3a, \cdots, (h-1)a. \tag{93}$$

From (92) it is seen that

$$\begin{aligned} t^m\omega &\equiv t^m\pi^{r_v}t^m\rho^{\mu} \pmod{\mathfrak{P}^{r_v+1}} \\ &\equiv \rho^{\alpha r_v}\pi^{r_v}\rho^{\mu} \pmod{\mathfrak{P}^{r_v+1}} \\ &\equiv \rho^{\alpha r_v+\mu}\pi^{r_v} \pmod{\mathfrak{P}^{r_v+1}}, \end{aligned}$$

or

$$t^m\omega \equiv \omega\rho^{\alpha r_v} \pmod{\mathfrak{P}^{r_v+1}}.$$

It follows at once that

$$\omega - t^m\omega \equiv \omega(1-\rho^{\alpha r_v}) \pmod{\mathfrak{P}^{r_v+1}}.$$

Due to this congruence it is seen that $\omega - t^m\omega$ is *not* divisible by $\mathfrak{P}^{r_v+1}$. For in that case it would follow that $1-\rho^{\alpha r_v}$ is divisible by $\mathfrak{P}$, which would require that αr_v be a multiple of p^f-1. And this is not possible; for $r_v = p^l$ is relative prime to p^f-1, and α, one of the numbers of (93), is less than $p^f-1 = ha$.

From this discussion it follows that each of the elements (91), whose product is equal to the relative different of $\mathfrak{k}_v$ with respect to $\mathfrak{k}_t$, is divisible exactly by $\mathfrak{P}^{r_v}$, so that the relative different is divisible by $\mathfrak{P}^{r_v(h-1)} = \mathfrak{P}^{r_t-r_v}$, as is required by Theorem II.

THEOREM III. In a similar manner: *The relative different of* $\mathfrak{k}_{\bar{v}}$ *relative to* $\mathfrak{k}_v$ *is divisible by* $\mathfrak{P}^{\lambda(r_v - r_{\bar{v}})} = \mathfrak{p}_{\bar{v}}^{\lambda(p^{\bar{e}}-1)}$ *exactly, while the relative different of* $\mathfrak{k}_{\bar{v}}$ *relative to* $\mathfrak{k}_v$ *is*

$$\mathfrak{P}^{\bar{\lambda}(r_{\bar{v}} - r_{\bar{\bar{v}}})} = \mathfrak{p}_{\bar{\bar{v}}}^{\bar{\lambda}(p^{\bar{\bar{e}}}-1)}, \text{ etc.}$$

For, if $\omega_1, \omega_2, \cdots$ form a basis of all integers of $\mathfrak{k}_v$, then the elements of the realm relative to $\mathfrak{k}_v$ are ideals

$$\{\omega_1 - v\omega_1,\ \omega_2 - v\omega_2,\ \omega_3 - v\omega_3,\ \cdots\},$$

where v goes through the substitutions of g_v that do not occur in $g_{\bar{v}}$. But for a number ω of $\mathfrak{k}_{\bar{v}}$ the difference $\omega - v\omega$ is divisible by $\mathfrak{P}^{\lambda}$, with the result that $\mathfrak{P}^{\lambda}$ takes the place of $\mathfrak{P}$ in the previous discussion.

It has been shown (Art. 187, end), if $\mathfrak{K}$ and $\mathfrak{k}$ are any two realms where $\mathfrak{k}$ is a sub-realm of $\mathfrak{K}$, that the different of $\mathfrak{K}$ is equal to the product of the different of $\mathfrak{k}$ by the relative different of $\mathfrak{K}$ with respect to $\mathfrak{k}$. It follows that *the different of the Galois realm contains* $\mathfrak{P}$ *exactly to the* m*th power, where*

$$m = r_t - r_v + \lambda(r_v - r_{\bar{v}}) + \bar{\lambda}(r_{\bar{v}} - r_{\bar{\bar{v}}}) + \cdots.$$

In Art. 240 it was seen that the discriminant D of the Galois realm was equal to the Nth power of the different, so that D contains the prime ideal $\mathfrak{P}$ as a factor exactly to the Nm power.

On the other hand due to formula (41), which is

$$p = (\mathfrak{P} \cdot s_1\mathfrak{P} \cdot s_2\mathfrak{P} \cdot \cdots \cdot s_{n_z-1}\mathfrak{P})^{r_t}, \tag{41}$$

it is seen that every prime factor p, as often as it is contained in D, introduces $\mathfrak{P}$ to the r_t power in D, so that, if we put

$$r_t\mu = Nm,$$

then is μ the power to which p enters D as a factor. Accordingly, from the relation just written we have

$$\mu = n_t m.$$

It is thus seen that the discriminant of the Galois realm contains p as a factor to the μth power, where

$$\mu = n_t[r_t - r_v + \lambda(r_v - r_{\bar{v}}) + \bar{\lambda}(r_{\bar{v}} - r_{\bar{b}}) + \cdots]. \tag{95}$$

Due to the general theorem proved in articles 75, 77 and 92, it is seen that

$$p^{f_1(e_1-1)+f_2(e_2-1)+\cdots} \tag{96}$$

enters as a factor in D, if the decomposition of p into its prime ideal factors is

$$p = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\mathfrak{P}_3^{e_3}\cdots,$$

where $\mathfrak{P}_i$ is of degree f_i $(i=1, 2, \cdots)$; and it was proved that the power (96) was the highest power of p that enters D if none of the exponents e_i is divisible by p. Due to formula (41) it is seen that e_i $(i=1, 2, 3, \cdots)$ is equal to r_t and the number of the prime ideals $\mathfrak{P}$ is n_z, each ideal being of the fth degree. Accordingly, if r_t is not divisible by p, then μ must be identical with the power of p in (96). In fact under this condition there exist no-stroked branch realms and $\mathfrak{k}_v$ is identical with $\mathfrak{K}$, so that $r_v=1$ and $\mu=n_t(r_t-1)$, which value is identical with the exponent in (96), and that is with $f(r_t-1)n_z$. Since $fr_t=r_z$ [formula (40)] and $r_z n_z=N$, this number is

$$N - fn_z = N - f\frac{N}{r_z} = N - \frac{N}{r_t} = N\left[1 - \frac{1}{r_t}\right].$$

This case occurs necessarily if N, the degree of $\mathfrak{K}$, is not divisible by p.

A still more general formula for the factorization of p is given in Art. 256.

ART. **250.** There is an interesting theorem due to Minkowski [1] which may be introduced here, a theorem which has to do with the units of the Galois realm.

[1] Minkowski, *Gött. Nach.*, 1900, p. 90; *Collected Works*, Vol. I, pp. 316–319.

Since the conjugate of a number of the Galois realm is a number of this realm, it is clear that the conjugates of every unit of the Galois realm are units in this realm. Accordingly the question was raised and proved to be true by Minkowski, that the $s-1$ independent units, which occur in the general theorem of Dirichlet (Arts. 111 ff., where the s here is the ν of that article) and through the composition of which all other units of a realm may be expressed, may, in the case of the Galois realm, be chosen as units conjugate among themselves.

If among the n conjugate realms $\mathfrak{R}^{(1)}$, $\mathfrak{R}^{(2)}$, $\cdots$, $\mathfrak{R}^{(n)}$ there are r_1 real realms and $r_2=\dfrac{n-r_1}{2}$ pairs of conjugate imaginary realms, and if $s=r_1+r_2$, it was proved that there are $s-1$ independent units, through the product of powers of which all other units may be expressed.

If

$$F(x)=0 \tag{i}$$

is the equation which produces the Galois realm, then each of its roots is a rational function of an arbitrary one of the roots with rational coefficients. It follows that all the roots are either real or they are all in pairs conjugate imaginary. Hence the number s in the first case equals N; and in the second case this number is $N/2$. In the first case let

$$A_1, A_2, \cdots, A_s \tag{97}$$

be the roots of (i); and in the second case let one root of each pair of conjugate imaginary roots be denoted by A_i $(i=1, 2, \cdots, s)$.

The number A which produces the Galois realm is found in the first case among the roots (97); in the second case choice is so made of the roots that A is one of them. It is seen that the following equations are true:

$$A_h=f_h(A), \qquad A=\varphi_h(A_h) \qquad (h=1, 2, \cdots, s),$$

where f_h and φ_h denote rational functions. From these equations it follows that $A = \varphi_h[f_h(A)]$; and due to the irreducibility of equation (i), it follows also in general that

$$\varphi_h[f_h(A_k)] = A_k \qquad (h, k = 1, 2, \cdots, s). \tag{98}$$

Further, since $f_h(A)$ is a root of the irreducible equation (i), it follows that $f_h(A_k)$ is also a root of that same equation and accordingly

$$f_h(A_1),\ f_h(A_2),\ \cdots,\ f_h(A_s) \tag{99}$$

are s roots conjugate to A. Moreover, no two of these roots are equal or conjugate imaginary; for, were $f_h(A_k)$ and $f_h(A_i)$ two such roots, then also must this be true of $\varphi_h(f_h(A_k))$ and $\varphi_h(f_h(A_i))$ and that is of A_k and A_i which is contrary to the choice of values (97). Accordingly the absolute values of the quantities (99) must be equal to those of (97).

Next let ϵ be a unit of the Galois realm, which being a number of this realm is equal to a rational function of A, say

$$\epsilon = \psi(A).$$

Accordingly

$$\epsilon_1 = \psi(A_1),\ \epsilon_2 = \psi(A_2),\ \cdots,\ \epsilon_s = \psi(A_s)$$

are the conjugates of ϵ, which correspond to (97).

On the other hand

$$\epsilon_h = \psi(A_h) = \psi[f_h(A)]$$

is also a unit of the Galois realm and

$$\psi[f_h(A_1)],\ \psi[f_h(A_2)],\ \cdots,\ \psi[f_h(A_s)] \tag{100}$$

are the conjugate units that correspond to the values (97). In view of what was said regarding (97) and (99) the absolute values of the quantities in (100) must be equal to those of the conjugate quantities $\epsilon_1, \epsilon_2, \cdots, \epsilon_s$.

Now we may so choose the unit ϵ, which due to the Dirichlet theory (Art. 121) is always possible, that the

conjugate value, which is taken as $\psi(A)$, is in absolute value greater than unity, while the remaining conjugate values are in absolute value less than unity. Then for the unit ϵ_h there will correspond a single one of the conjugates, namely that number of the series (100) in which $f_h(A_i)$ is the equal of, or the conjugate imaginary of A, when $A_i = \varphi_h(A)$. The absolute value of this unit is greater than unity, while the absolute values of all its conjugates are less than unity; and further these conjugate values, due to (97), for $h=1, 2, \cdots, s$ must be different from one another, since the same A_i cannot be equal to, or be the conjugate imaginary of two of the quantities

$$\varphi_1(A), \ \varphi_2(A), \ \cdots, \ \varphi_s(A).$$

Also observe, as h goes through the series $1, 2, \cdots, n$, that the first of the conjugate values chosen above corresponds to another of the values (97).

From this it is evident that any $s-1$ of the conjugate units

$$\epsilon_1, \ \epsilon_2, \ \cdots, \ \epsilon_s$$

are just such $s-1$ units of the Galois realm as are required (Art. 111) to constitute a system of independent units.

Accordingly, we have proved the theorem: *In the Galois realm there is always a unit such that every unit of the realm may be expressed as a product of this unit and its conjugates, with rational integral exponents.*

EXAMPLES

1. In the Kronecker Theory, *Grundzüge*, p. 33, every algebraic realm may be made a sub-realm of a Galois realm. Find the modification that must be made in the units as determined above in the Galois realm to obtain a fundamental set of units for the algebraic realm in question.

2. Using Hilbert's Theorem 39, prove that the Galois realm that is compounded of any algebraic realm $\mathfrak{k}$ and its conjugates, has as divisors of its discriminant only the rational prime integers which divide the discriminant of $\mathfrak{k}$.

3. Two realms of degrees n_1 and n_2 whose discriminants are relative prime, when compounded, produce a realm of degree $n_1 n_2$.

4. Two realms of degrees n_1 and n_2 with discriminants d_1 and d_2 that are relative prime, when compounded, offer a discriminant whose value is $d_1^{n_2} d_2^{n_1}$. (See Hensel, *Crelle*, Vol. 105, pp. 329 ff.)

CHAPTER XVI

DEVELOPMENT OF ALGEBRAIC NUMBERS IN SERIES. THE p-ADIC NUMBERS

ART. **251.** We shall give here a cursory discussion of Hensel's method [1] of treating algebraic numbers by means of series (p-adic numbers) and in particular the factorization of the discriminant of a given realm $\Re(\omega)$.

Let $\Re(\omega)$ be a given realm of the nth degree which is produced by the integer ω and let $\omega_1, \omega_2, \cdots, \omega_n$ denote the integers conjugate with and including ω. In this realm let

$$p = \mathfrak{p}_1^{e_1} \cdot \mathfrak{p}_2^{e_2} \cdot \mathfrak{p}_3^{e_3} \cdot \cdots \tag{1}$$

be the factorization of the rational prime integer p into its prime ideal factors $\mathfrak{p}_1, \mathfrak{p}_2, \cdots$ of degrees $f_1, f_2, \cdots$ respectively. Denote by $\mathfrak{p}^e$ the power of any one of these prime ideal factors of p and let f denote the degree of $\mathfrak{p}$.

Then (see Art. 64, or Hilbert, Theorem 29) note that every integer of $\Re(\omega)$ is congruent (mod. $\mathfrak{p}^m$) to a definitely determined expression of the form

$$A_0 + A_1\pi + A_2\pi^2 + \cdots + A_{m-1}\pi^{m-1}, \tag{2}$$

where the primitive number π is divisible by $\mathfrak{p}$ but not by $\mathfrak{p}^2$. The quantities A_i may be written in the form

$$A_i = a_{i0} + a_{i1}\rho + a_{i2}\rho^2 + \cdots a_{i,f-1}\rho^{f-1} \quad (i = 0, 1, \cdots, m-1), \tag{3}$$

[1] This chapter is taken for the most part from Hensel, "Ueber die Entwicklung der algebraischen Zahlen in Potenzreihen," *Math. Annalen*, Vol. 55, pp. 30 ff. See Hensel, "Neue Grundlagen der Arithmetik," *Crelle*, Vol. 127, p. 50; and Hensel, "Ueber eine neue Begrundung der Theorie der algebraischen Zahlen," *Crelle*, Vol. 128, p. 1. See also Bauer, *Math. Zeitsch.*, Vol. 16, pp. 1 ff.

This theory was worked over by Bachmann, *Allg. Arithmetik*, pp. 521 ff. An excellent account of p-adic numbers with numerous references by Wahlin is found in the *Report on Algebra ic Numbers*, §§ 21–38.

where the a's can take all values from 0 to $p-1$. Further ρ is a root of an irreducible (mod. p) congruence

$$P(x)\equiv 0 \pmod{\mathfrak{p}} \tag{4}$$

of degree f, whose coefficients are rational integers, reduced (mod. p). If $\gamma=\tau/\sigma$ is fractional, determine k, so that $\tau\pi^k=\sigma\lambda=\mu$, or $\gamma\pi^k=\lambda$, where τ, σ, μ, λ are integral (Vol. I, p. 380). It follows that γ is of the form (2), although the expression may begin with negative powers of π. It is seen that for any number ζ of $\Re(\omega)$ and for an integral value of m, arbitrarily large, the following congruence exists:

$$\zeta\equiv A_r\pi^r+A_{r+1}\pi^{r+1}+\cdots+A_{m-1}\pi^{m-1} \pmod{\mathfrak{p}^m}, \tag{2a}$$

where the exponent r is called the *order* of ζ (mod. $\mathfrak{p}$) and is a rational integer, positive, negative, or zero.

It is clear (Art. 63) that the number ρ may be replaced by any congruent (mod. $\mathfrak{p}$) integral expression

$$\bar{\rho}=\rho+a_1\pi+a_2\pi^2+\cdots, \tag{5}$$

and the number π through any integral expression

$$\bar{\pi}=b_1\pi+b_2\pi^2+b_3\pi^3+\cdots. \tag{6}$$

Here b_1 is relative prime to p, since $\bar{\pi}$ must not be divisible by $\mathfrak{p}^2$.

By making use of such substitutions it is possible to determine a new integer $\bar{\rho}$ which satisfies the congruence (4) not only (mod. $\mathfrak{p}$) but also for any arbitrarily large power of $\mathfrak{p}$ as modulus. Observe first that the number ρ which satisfies the congruence (4) cannot also satisfy

$$P'(\rho)\equiv 0 \pmod{\mathfrak{p}}.$$

For since the irreducible (mod. p) function $P(x)$ is relative prime to $P'(x)$, we may always determine a congruence

$$P(x)\varphi(x)+P'(x)\psi(x)\equiv 1 \pmod{p},$$

which shows that $P(x)$ and $P'(x)$ are not simultaneously divisible by p.

Suppose next that $\bar{\rho}$ has been so chosen that $P(\bar{\rho})$ is exactly divisible by $\mathfrak{p}^l$ where $l \geqq 1$, and consequently $P(\bar{\rho})$ has the form

$$C_l\pi^l + C_{l+1}\pi^{l+1} + \cdots.$$

If then $\bar{\rho}$ is replaced by $\bar{\rho} + A\pi^l$ it is seen that

$$\begin{aligned} P(\bar{\rho} + A\pi^l) &= P(\bar{\rho}) + A\pi^l P'(\bar{\rho}) + \cdots \\ &= \pi^l[C_l + AP'(\bar{\rho})] + \cdots. \end{aligned}$$

Since $P'(\bar{\rho})$ is not divisible by $\mathfrak{p}$, we may so choose A that $C_l + AP'(\bar{\rho})$ is divisible by $\mathfrak{p}$. Hence writing $\bar{\rho} + A\pi^l = \bar{\rho}^*$, it is clear that $P(\bar{\rho}^*)$ is divisible by $\mathfrak{p}^{l+1}$; and continuing this process it is seen that an integer may be determined, say x, such that $P(x)$ is divisible by an arbitrarily high power of $\mathfrak{p}$.

Further, the number π may be replaced, as follows, by a value $\bar{\pi}$ which is more suitable for our purposes. Since π is exactly divisible by $\mathfrak{p}$ and p by $\mathfrak{p}^e$, it is seen that $\frac{\pi^e}{p}$ is (mod. $\mathfrak{p}$) of the order zero, and we may put

$$\begin{aligned} \frac{\pi^e}{p} = -[B_0 + B_1\pi + B_2\pi^2 + \cdots + B_{e-1}\pi^{e-1}] \\ + B_e\pi^e + B_{e+1}\pi^{e+1} + \cdots \pmod{\mathfrak{p}^m}, \end{aligned}$$

where the quantities B_i belong to the realm $\mathfrak{R}(\rho)$ and $B_0 \not\equiv 0$. Hence, writing

$$\frac{\pi^e}{p} + B_0 + B_1\pi + \cdots + B_{e-1}\pi^{e-1} = B',$$

we observe that (mod. $\mathfrak{p}$) B' is at least of the order e. Further and in a similar manner, writing

$$\frac{B'}{p} + B'_0 + B'_1\pi + B'_2\pi^2 + \cdots + B'_{e-1}\pi^{e-1} = B'',$$

it is seen that B'' is at least of the order e; and continuing

$$\frac{B''}{p}+B_0''+B_1''\pi+\cdots+B_{e-1}''\pi^{e-1}=B'''$$

is at least of the order e; etc.

Observe that

$$\begin{aligned}
pB' &= \pi^e \quad +pB_0+pB_1\pi+\cdots+pB_{e-1}\pi^{e-1},\\
p^2B'' &= pB' +p^2B_0'+p^2B_1'\pi+\cdots+p^2B_{e-1}'\pi^{e-1},\\
p^3B''' &= p^2B''+p^3B_0''+p^3B_1''\pi+\cdots+p^3B_{e-1}''\pi^{e-1},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots.
\end{aligned}$$

Writing

$$pC_i=pB_i+p^2B_i'+p^2B_i''+\cdots \tag{7}$$

and adding the above expressions, it is clear that

$$\Phi(\pi)=\pi^e+pC_{e-1}\pi^{e-1}+pC_{e-2}\pi^{e-2}+\cdots+pC_0\equiv 0 \pmod{\mathfrak{p}^m}. \tag{8}$$

It is thus proved that π is a root of a congruence

$$\Phi(x)\equiv 0 \pmod{\mathfrak{p}^m}, \tag{9}$$

whose coefficients, except the first one (which is unity), are all divisible by p, while the last coefficient

$$pC_0=pB_0+p^2B_0'+p^3B_0''+\cdots$$

is not divisible by powers of p higher than the first. Thus applying the theorem of Schönemann (Vol. I, Art. 11), which is also applicable for algebraic integers, it is seen that the function $\Phi(x)$ is irreducible in the realm $\Re(\rho)$, the realm to which the coefficients of $\Phi(x)$ belong. Observe that the greater the power of $\mathfrak{p}$ and the farther the series (7) advances, the larger are the values of the coefficients C_i. It is possible, however, to replace the number π, according to which the series is developed, by another number of the form (6) for which in contradistinction the coefficients C_i remain below a finite limit, however high the power $\mathfrak{p}^m$ is chosen. (See Hensel, *Theorie der algebraischen Zahlen*, Chapt. II, § 5.)

Observe that the single terms which constitute the function $\Phi(\pi)$ in its development in formulas (8) and (7), that is, terms of the form

$$p^h B_i^{(h-1)} \pi^t,$$

when present, are, with respect to $\mathfrak{p}$ of the order $he+i$. All these individual terms are of different orders (mod. $\mathfrak{p}$) excepting the two terms π^e and pB_0, which are of the same order. Observe that this is also true of the derivatives of $\Phi(\pi)$, and that is, of

$$(10) \qquad \frac{\Phi'(\pi)}{1}, \frac{\Phi''(\pi)}{2!}, \frac{\Phi'''(\pi)}{3!}, \cdots, \frac{\Phi^{(e)}(\pi)}{e!}.$$

Next consider those terms in $\Phi(\pi)$, whose orders are less than or equal to k, where k is a number determined later. Let these terms constitute the function $\Psi(\pi)$, so that

$$\Phi(\pi) = \Psi(\pi) + \mathrm{X}(\pi),$$

where the terms of $\mathrm{X}(\pi)$ are of order higher than k. It follows that

$$(11) \qquad \Psi(\pi) \equiv D_l \pi^l + D_{l+1} \pi^{l+1} + \cdots \pmod{\mathfrak{p}^m},$$

where $l > k$. Next write $\overline{\pi} = \pi + \lambda \pi^r$, where λ is *not* divisible by $\mathfrak{p}$. It follows that

$$(12) \quad \Psi(\overline{\pi}) = \Psi(\pi) + \lambda \pi^r \Psi'(\pi) + (\lambda \pi^r)^2 \frac{\Psi''(\pi)}{2!} + \cdots$$
$$= D_l \pi^l + D_{l+1} \pi^{l+1} + \cdots + \lambda \pi^r \Psi'(\pi) + \cdots.$$

Suppose that the orders of $\Psi^{(i)}(\pi)$ $(i=1, 2, \cdots, e)$ are respectively $\rho_1, \rho_2, \cdots, \rho_e$. Hence the terms to the right in (12) are respectively of orders

$$l, l+1, \cdots, \rho_1 + r, \rho_2 + 2r, \cdots, \rho_e + er.$$

Suppose next that r_0 is the smallest integer for which

$$\rho_1 + r_0 < \rho_i + i r_0 \qquad (i=2, 3, \cdots, e),$$

so that consequently r_0 is greater than all the numbers

$$\frac{\rho_1 - \rho_i}{i-1} \qquad (i=2, 3, \cdots, e).$$

Hence for every number r which is $\geqq r_0$ there exist the inequalities

$$\rho_1 + r < \rho_i + ir \qquad (i=2, 3, \cdots, e);$$

and consequently due to (12) we may put

$$\Psi(\bar{\pi}) = \Psi(\pi) + C\lambda\pi^{r+\rho_1} + \cdots \tag{13}$$
$$= (D_l\pi^l + \cdots) + C\lambda\pi^{r+\rho_1} + \cdots,$$

where $C\lambda\pi^{r+\rho_1}$ is the term of lowest order in $\lambda\pi^r\Psi'(\pi)$, all the following terms being of higher order.

The rational integer r_0+r_1-1 is fixed, dependent only upon the expressions (10), and is independent of the distribution of $\Phi(\pi)$ into its two component sums of $\Psi(\pi)$ and $\mathrm{X}(\pi)$.

We shall choose it for the number k introduced above. It follows that $l \geqq r_0+\rho_1$. Hence if we choose $r+\rho_1=l$, it follows that $r \geqq r_0$, which condition must be satisfied. In this case the right hand side of (13) begins with a term of lowest order

$$(D_l + C\lambda)\pi^l.$$

Since C is not divisible by $\mathfrak{p}$, a suitable choice of λ can be made within $\mathfrak{R}(\omega)$, so that $D_l+C\lambda$ is divisible by π. As the same process may be repeated without altering the value of k, it is evident that by the introduction of numbers $\bar{\bar{\pi}} = \bar{\pi} + \lambda'\pi^{r'}$, etc., in the place of $\bar{\pi}$, etc., any number of further terms in (11) may be made to disappear.

In other words, instead of π another number $\bar{\pi}$ of the form (6) may be found such that the congruence

$$\Psi(\bar{\pi}) \equiv 0$$

is satisfied with respect to any arbitrarily high power $\mathfrak{p}^m$ as modulus.

The left hand side of this expression consists of a finite number of terms that have been previously fixed and determined through k. It is thus proved [1] that *every*

[1] Cf. Hensel, *Math. Ann.*, 55, p. 306.

number ζ of $\Re(\omega)$ with respect to an arbitrarily high power of $\mathfrak{p}$ as modulus, may be uniquely expressed in the form of a series

$$\zeta = A_r\pi^r + A_{r+1}\pi^{r+1} + \cdots \pmod{\mathfrak{p}^m}. \tag{14}$$

The two numbers ρ and π, the development numbers, which appear in this expansion, may be so chosen that ρ satisfies the congruence

$$P(x) \equiv 0 \pmod{\mathfrak{p}^m}, \tag{15}$$

while π satisfies the congruence

$$\Psi(x) \equiv 0 \pmod{\mathfrak{p}^m}. \tag{16}$$

The function $\Psi(x)$ has the form

$$\Psi(x) = x^e + p\overline{C}_{e-1}x^{e-1} + \cdots + p\overline{C}_0, \tag{17}$$

where the coefficients $p\overline{C}_i (i = 0, 1, \cdots, e-1)$ are expressions of the form (7), with the restriction that, however great m may be taken, these coefficients do not exceed a fixed degree with respect to p. And therefore after a definitely determined value of m has been reached, the congruence (16), as also the congruence (15), remain unchanged.

It is clear that the integer π may be replaced by any other integer that is congruent to it (mod. $\mathfrak{p}^m$). We may assume that π is divisible by none of the other prime ideal factors of p; for it is possible to form an integer which is divisible by $\mathfrak{p}$ and which is congruent to 1 with respect to every other prime ideal factor of p as modulus (Vol. I, Art. 143).

If e is not divisible by p, it may be shown as follows that $\Psi(x)$ takes the simple form

$$\Psi(x) = x^e + pB_0,$$

where B_0, as indicated above, is not divisible by $\mathfrak{p}$ and is an integer in $\Re(\omega)$. For under the given hypothesis it is seen that in

$$\Psi'(x) = e\pi^{e-1} + p(e-1)C_{e-1}\pi^{e-2} + \cdots + pC_1,$$

the term of lowest order is the first one; and its order is $e-1$, since the other terms all contain the factor p and are therefore at least divisible by $\mathfrak{p}^e$. We therefore have $\rho_1 = e-1$. In the same way it is seen, for $i>1$, that

$$\rho_i \geqq e-i.$$

Accordingly, we have

$$\frac{\rho_1-\rho_i}{i-1} \leqq \frac{(e-1)-(e-i)}{i-1} = 1 \qquad (i=2, 3, \cdots, e);$$

and, as r_0 is the smallest integer for which

$$\rho_1 + r_0 < \rho_i + ir_0 \qquad (i=2, 3, \cdots, e),$$

it is seen that we may take $\rho_0 = 2$. It follows that $k = r_0+\rho_1-1 = e$, and then through the method as given in formula (13) all terms of order higher than e may be eliminated, thus leaving the terms π^e and pB_0.

ART. **252.** Only *exceptionally* does the left hand side of (16) take the more general form (17), and this happens when e is divisible by p, which occurs in a finite number of cases, due to the fact that $e=1$, unless p is a divisor of the discriminant of the realm (Arts. 30 and 102). And this is the kern of the entire investigation that is here considered. Up to this time these singular cases offered an anomaly, which could not be overcome, while here there is no exception to the results that follow later. (See Hensel, *Math. Ann.*, 55, p. 306.)

The results of the preceding article have been derived by means of the ideal theory for an arbitrarily high power of a prime ideal factor $\mathfrak{p}$ of a real prime integer p as modulus. (See Bachmann, *Allgemeine Arithmetik*, etc., p. 521.)

In an analogous manner, but independent of the ideal theory, the same results have been established by Hensel " Ueber eine neue Begrundung der Theorie der alge-

braischen Zahlen." (*Jahresberichte der deutschen math. Vereinigung*, Vol. 6, p. 83.)

The foundations of this theory are laid upon the simple notion that just as every positive integer with respect to a prime number p may be expressed in the form of a *finite* power-series

$$a_0+a_1p+a_2p^2+\cdots,$$

where the a's are reduced (mod. p), being consequently found among the numbers 0, 1, 2, $\cdots$, $p-1$, so also every negative or fractional number may be expressed as an *infinite* series similar to the above, where the question is not regarding the value of this negative or fractional number, but regarding its residue with respect to an arbitrarily high power of p. In this sense Hensel extended the realm of all rational numbers to the realm of infinite series

$$a_0+a_1p+a_2p^2+\cdots$$

with arbitrary, but definitely given coefficients, reduced (mod. p). He also developed the arithmetic theorems for *number-quantities* (*Zahlengrössen*) of this sort as well as for integral algebraic functions of one variable, in which functions these number-quantities appear as coefficients; and Hensel then showed that similar methods of presentation exist for the algebraic numbers as they do for the rational numbers. He further showed from these expansions in series, how it is possible to determine whether a number is divisible by an integral or fractional power of p or through the power of a prime ideal.

It has been shown for every number ζ of $\Re(\omega)$, that there exists an expansion in series of the form

$$\zeta=A_r\pi^r+A_{r+1}\pi^{r+1}+\cdots, \tag{18}$$

where r is an integer, which may be positive, negative, or

zero, and where

$$A_i = a_{0i} + a_{1i}\rho + \cdots a_{f-1,i}\rho^{f-1}.$$

In this expression ρ is the root of an irreducible equation (mod. p) of the fth degree, say

$$P(x) = 0,$$

with coefficients that are reduced (mod. p). And finally π is the root of an equation of the form (17)

$$\Psi(x) = 0.$$

For the usual prime integer p, by which we mean one that is not a divisor of the discriminant of $\Re(\omega)$, we have $\pi = p$; and the development in series (18) is of the form

$$(18a) \qquad \zeta = \frac{A_{-h}}{p^h} + \cdots + \frac{A_{-1}}{p} + A_0 + A_1 p + \cdots.$$

Such a series is called a *regular* p-adic one. For brevity, we shall define such a development series as " belonging to the position (p, ω) " (see Hensel-Landsberg, *Algebraischen Funktionen einer Variabelen*, p. 29).

Only for those prime integers which are divisors of the discriminant is π a " sort of root " of p, or more precisely " an associate " of such a root. For writing $\pi = p\tilde{\omega}^{\frac{1}{e}}$, it is seen from (17), π being a root of that expression, that $\tilde{\omega}$ satisfies an equation

$$(19) \quad \tilde{\omega}^e + p^{\frac{e-1}{e}} C_{e-1}\tilde{\omega}^{e-1} + p^{\frac{e-2}{\omega}} C_{e-2}\tilde{\omega}^{e-2} + \cdots + C_0 = 0,$$

and therefore is an algebraic integer. In fact since C_0 is not divisible by p, it, and with it $\tilde{\omega}$, may be regarded as units (mod. p). It may be observed that by definition $C_0 = B_0 + pB_0' + p^2 B_0'' + \cdots$. Hence the series (18), or otherwise written,

$$(18b) \quad \zeta = \frac{A_{-h}}{\pi^h} + \frac{A_{-h+1}}{\pi^{h-1}} + \cdots + \frac{A_{-1}}{\pi} + A_0 + A_1\pi + \cdots$$

may be developed for the prime integer in question p, in ascending powers of $p^{\frac{1}{e}}$.

Since $p^{\frac{1}{e}}$ has e conjugate values different through multiples of the eth roots of unity, the formula (18b) presents collectively a complex of e different values of ζ, which are conjugate to one another.

To the *singular position* (p, ω) there correspond e conjugate developments in series; and precisely as in the theory of algebraic functions there is in the neighborhood of a singular or branch-point a number of different branches that belong to the function.

On this account the position (p, ω) may be called a *branch-position* of the $(e-1)$st order, so that a regular position may be counted as of the zero order.

On the other hand the number ρ which appears in the coefficients A_i, being a root of an equation $P(x)=0$ of the fth degree, may have f different values; and it is seen that each of the equations (18a) or (18b) may have exactly f different expansions. This, combined with the above, shows that there may be e development in series, through which every f of the conjugate values of ζ may be given.

A comparison of these theorems with the results of the previous article indicates the connection with the theory of ideals. For corresponding to every branch point of the $e-1$st order, in which appear f connected complexes, where each complex may be expanded in e series, there exists a prime ideal factor $\mathfrak{p}$ of p, whose degree is f and which appears as a factor to the eth power in p. Since $e=1$ except for the prime numbers p which are divisors of the discriminant of the stock-realm, it is seen that for all the remaining prime numbers, the branch-points are regular and the developments are of the form (18a).

Observe that the order of the development (18) is the exponent r of the power π^r and is a positive or negative integer (including zero). The order gives the exact power $\mathfrak{p}^r$ of the prime ideal $\mathfrak{p}$, through which ζ is divisible and for which ζ/π^r is integral. It is further evident that to every other prime ideal factor $\mathfrak{p}'$, which occurs to the e' power as a factor of p, and whose degree is f', there corresponds a branch-point of the $e'-1$ order, at which there are united f' complexes, and where for each complex there appear e' different series of an analogous nature as are the series (18b), so that to the previous ef conjugate values of ζ there must be added $e'f'$ additional values. By continuing this process it is clear that

$$ef+e'f'+\cdots=n.$$

Through these theorems Hensel established a complete analogy between the theory of ideals and the theory of algebraic functions. These results he extended in two papers published in the *Gött. Nachr.*, 1897. One has to do with the fundamental equation (Art. 71) and the other with the exact composition of the discriminant, and in particular with the *singular* divisors of the discriminant. This latter with the further investigation due to Hensel we shall consider in the sequel. Hensel's paper "Ueber die Entwicklung der algebraischen Zahlen in Potenzreihen" (*Math. Annal.*, Vol. 55, p. 301) is particularly of fundamental importance. (See also Hensel, *Theorie der algebraischen Zahlen*, Chapt. XII.)

ART. **253.** Consider the equation

$$P(x)=0, \tag{20}$$

which in Art. 251 was assumed to be irreducible (mod. p), and which for a greater reason is irreducible here. Let

$$\rho_1, \rho_2, \cdots, \rho_f$$

be its roots.

Further let the irreducible function $\Psi(x)$, whose coefficients belong to the realm $\Re(\rho)$, be denoted by $\Psi_k(x)$, when ρ is changed with ρ_k; and let

(21) $$\pi_{k1},\ \pi_{k2},\ \cdots,\ \pi_{ke}$$

be the roots of the irreducible equation

(22) $$\Psi_k(x)=0 \qquad (k=1, 2, \cdots, f)$$

in the realm $\Re(\rho_k)$.

The collectivity of all numbers constituted rationally out of ρ_1 and π_{11} form a realm of rationality $\Re(\pi_{11}, \rho_1)$, which is of degree ef. Observe that the ef numbers

(23) $$\rho_1^g \pi_{11}^h \qquad \begin{pmatrix} g=0, 1, \cdots, f-1 \\ h=0, 1, \cdots, e-1 \end{pmatrix}$$

form a basis of this realm. The realms which are conjugate with this realm are

$$\Re(\pi_{kh}, \rho_k) \qquad \begin{pmatrix} k=1, 2, \cdots, f \\ h=1, 2, \cdots, e \end{pmatrix}.$$

Take any Galois realm $\mathfrak{K}_g$ which contains all these ef conjugate realms and also the stock-realm $\Re(\omega)$, and let $\mathfrak{P}$ denote any prime ideal factor in $\mathfrak{K}_g$ through which the ideal $\mathfrak{p}$ of Art. 251 is divisible. Hence the congruences (15) and (16) of Art. 251 also exist for $\mathfrak{P}^m$, and that is

$$P(x)\equiv 0 \pmod{\mathfrak{P}^m} \quad \text{and} \quad \Psi(x)\equiv 0 \pmod{\mathfrak{P}^m};$$

and proceeding with $\mathfrak{P}$ as modulus, instead of $\mathfrak{p}$, as in article 251, it is seen that

(24) $$\rho\equiv\rho_1, \qquad \pi\equiv\pi_{11} \pmod{\mathfrak{P}^m},$$

where ρ and π are the *development numbers* in the extended realm $\mathfrak{K}_g$, and where m is arbitrarily large.

Hence every number of the realm $\Re(\omega)$ is congruent (mod. $\mathfrak{P}^m$) to a number of the form

(25) $$A_r\pi_{11}^r+A_{r+1}\pi_{11}^{r+1}+\cdots,$$

where the A's are integral functions of ρ_1 with rational integral coefficients; and in particular the number ω,

which determines the initial stock-realm $\Re(\omega)$, satisfies the congruence

$$\omega \equiv \omega^{(0)} \pmod{\mathfrak{P}^m}, \tag{26}$$

where $\omega^{(0)}$ is a definite number of the form (25). At the same time every integral number of $\Re(\omega)$, as a rational function $\varphi(\omega)$ of ω, is congruent (mod. $\mathfrak{P}^m$) to the corresponding (also integral) number $\varphi(\omega^{(0)})$ of the realm $\Re(\pi_{11}, \rho_1)$; and in this sense the entire realm $\Re(\omega)$ is *imaged* (*abgebildet*) on the realm $\Re(\pi_{11}, \rho_1)$. This relation is also reversible;[1] for simultaneously with the congruence of the numbers ρ_1, π_{11} with ρ, π it is clear that every integral number that is rationally formed of ρ_1, π_{11} is also congruent to the integral number that is formed of ρ, π.

It may be proved next that *a congruence of the form*

$$\sum_{\varrho=0}^{f-1} \sum_{h=0}^{e-1} a_{\varrho h} \rho_1^{\varrho} \pi_{11}^{h} \equiv 0 \pmod{\mathfrak{P}^m}, \tag{27}$$

or more simply a congruence

$$A_0 + A_1\pi_{11} + A_2\pi_{11}^2 + \cdots + A_{e-1}\pi_{11}^{e-1} \equiv 0 \pmod{\mathfrak{P}^m}, \tag{28}$$

where the A's are integral functions of ρ_1 with integral coefficients, can exist only identically, and that is, each term of the double summation is of itself divisible by the modulus.

To prove this, determine the highest power of p which divides all the A's in (28). If it contains the prime factor $\mathfrak{P}$ to a power higher than m, the congruence (27) exists identically. In the other event through division by the highest power of $\mathfrak{P}$ there exists a congruence

$$A'_0 + A'_1\pi_{11} + A'_2\pi_{11}^2 + \cdots + A'_{e-1}\pi_{11}^{e-1} \equiv 0 \pmod{\mathfrak{P}^{m'}}, \tag{29}$$

in which some of the A's are not divisible by p. It

[1] Read pp. 236 et seq. of the *Theorie der algebraischen Funktionen einer Variabeln*, by Hensel and Landsberg.

follows from the equation

(30) $\pi_{11}^{e}+p(C_{e-1}\pi_{11}^{e-1}+\cdots+C_0)=0$ [see formula (8)],

which equation is satisfied by π_{11}, that the prime ideal divisor $\mathfrak{P}$ of p is a divisor of π_{11}; and, if it appears to the δ power in π_{11}, it must enter to the $e\delta$ power in p, since C_0 is relative prime to p. If then A'_h is the first of the series $A'_0, A'_1, \cdots$ that is not divisible by p, and if $m' \geqq h\delta$, then is every term in (29) of itself divisible by $\mathfrak{P}^{m'}$, and the congruence (27) is identically satisfied. It may be proved that the assumption $m' > h\delta$ is not permissible. For the congruence (29), when considered with respect to the modulus $\mathfrak{P}^{h\delta+1}$, reduces to the simpler form

$$A'_h\pi_{11}^{h} \equiv 0 \text{ (mod. } \mathfrak{P}^{h\delta+1}),$$

the terms preceding this term all being divisible by p and therefore by $\mathfrak{P}^{e\delta}$, where $e\delta \geqq h\delta+1$, while the following terms are all divisible by π_{11}^{h+1}, and that is by $\mathfrak{P}^{(h+1)\delta}$. In the term $A'_h\pi_{11}^{h}$, since π_{11}^{h} is divisible by $\mathfrak{P}^{h\delta}$, it is clear that A'_h must be divisible by $\mathfrak{P}$, and on account of the irreducibility (mod. p) of equation (20), which ρ_1 satisfies, it follows that A'_h must be divisible by p, which is contrary to the assumption previously made.

From this it is seen in particular that *the basal elements (23) of the "image" realm form a fundamental system (mod. p) for this realm, and that is that a congruence*

$$(31) \qquad \sum_{g=0}^{g=f-1}\sum_{h=0}^{h=e-1} a_{gh}\rho_1^{g}\pi_{11}^{h} \equiv 0 \text{ (mod. } p)$$

with rational or integral coefficients, or more simply a congruence

$$(32) \quad A_0+A_1\pi_{11}+A_2\pi_{11}^{2}+\cdots+A_{e-1}\pi_{11}^{e-1} \equiv 0 \text{ (mod. } p),$$

in which the A's are integral functions of ρ_1 with integral coefficients and of degree $f-1$, is only possible, if the coefficients a_{gh} or A_i are all divisible by p.

For the congruence (32) offers the following congruence

$$(32a) \quad A_0+A_1\pi_{11}+A_2\pi_{11}^2+\cdots+A_{e-1}\pi_{11}^{e-1}\equiv 0 \pmod{\mathfrak{P}^{e\delta}},$$

which requires that every single term be divisible by $\mathfrak{P}^{e\delta}$, and that is, every coefficient A must be divisible by $\mathfrak{P}$ and therefore also by p.

Due to the two theorems above we may conclude that *the number $\omega^{(0)}$—at least for sufficiently large values of m—is of the same degree ef as the image realm to which it belongs.*

For let $m \geqq e\delta$, and let

$$(33) \qquad \psi(x)\equiv 0 \pmod{\mathfrak{P}^{e\delta}}$$

be the congruence with integral coefficients and of least degree which $\omega^{(0)}$ satisfies. Its degree ν can not be greater than the degree of $\omega^{(0)}$ and that is of the degree of the irreducible equation

$$(34) \qquad \mathrm{X}(x)=0,$$

which $\omega^{(0)}$ satisfies. For if the equation $\mathrm{X}(\omega^{(0)})$ exists, then for a greater reason we have $\mathrm{X}(\omega^{(0)})\equiv 0 \pmod{\mathfrak{P}^{e\delta}}$. And this degree is not greater than ef, as $\omega^{(0)}$ is a number belonging to a realm of this degree, namely, the image realm. It is proved below that ν is not less than ef and consequently the degree of the equation (34) cannot be less than ef. It follows that $\nu=ef$. To prove that ν is *not* less than ef, make the assumption that the contrary is the case, and that is, $\nu<ef$. Since each of the numbers

$$\rho_1^g\pi_{11}^h \qquad \begin{pmatrix} g=0,\,1,\,2,\,\cdots,\,f-1 \\ h=0,\,1,\,2,\,\cdots,\,e-1 \end{pmatrix}$$

is congruent (mod. $\mathfrak{P}^m$) and therefore also (mod. $\mathfrak{P}^{e\delta}$) to an integer $\varphi(\omega)$ of $\mathfrak{R}(\omega)$, and therefore also to a corresponding integer $\varphi(\omega^{(0)})$ of the image realm, it follows, due to the identity

$$\psi(\omega^{(0)})\equiv 0 \pmod{\mathfrak{P}^{e\delta}}$$

of degree ν, that for each of the above numbers there

exists a relation of the form

$$\rho_1^{g}\pi_{11}^{h} \equiv r + r_1\omega^{(0)} + \cdots + r_{\nu-1}\omega^{(0)^{\nu-1}} \pmod{\mathfrak{P}^{e\delta}}$$

with rational coefficients. Let n_{gh} be the least common multiple of the denominators of the fractional coefficients. It follows that

$$(35) \quad n_{gh}\rho_1^{g}\pi_{11}^{h} \equiv a + a_1\omega^{(0)} + \cdots + a_{\nu-1}\omega^{(0)^{\nu-1}} \pmod{\mathfrak{P}^{e\delta}},$$

where the a's are integers which do not all have a common divisor with n_{gh}. Observe that n_{gh} cannot be divisible by p, otherwise the right-hand member of (35) would be a non-identical congruence (mod. $\mathfrak{P}^{e\delta}$) which is satisfied by $\omega^{(0)}$ contrary to the assumption that ν was the least degree of such a congruence that is satisfied by $\omega^{(0)}$. If there existed a non-identical congruence of the form (27) or (28) derived through the elimination of $\omega^{(0)}$ from the ef congruences (35), we would have proved the inadmissibility of the assumption $\nu < ef$, since we have proved that there was no non-identical congruence of such a form.

We shall next prove that through such elimination there *does* exist such a congruence.

Consider any ν arbitrarily chosen of the congruences (35). Their determinant Δ cannot be divisible by $\mathfrak{P}$ or by p as Δ is a rational integer; otherwise, as in the case of linear equations, it would be possible to choose ν integers $c_1, c_2, \cdots, c_\nu$, which are not all divisible by p, such that when the right hand sides of the ν congruences in question are multiplied by $c_1, c_2, \cdots, c_\nu$ respectively, the sum of the resulting expressions would be divisible by p, and this would be equally true of the left hand side of the ν congruences, when multiplied by $c_1, c_2, \cdots, c_\nu$ respectively and added. And that is, this sum would be divisible by $\mathfrak{P}^{e\delta}$, thus offering a congruence of the form (32a), without all the coefficients being divisible by p.

Suppose next that Δ is prime to $\mathfrak{P}$. Then solving the ν congruences in question, it is seen that $\Delta\omega^{(0)_h}$ $(h=0, 1, \cdots, \nu-1)$ may be expressed linearly in terms of the ν quantities $n_{\varrho h}\rho_1^{\delta}\pi_{11}^{h}$ (mod. $\mathfrak{P}^{e\delta}$) with integral coefficients; and when these quantities are substituted in another one of the ef congruences (35), after this congruence has been multiplied by Δ, it is seen that a congruence of the form (32a) is brought into existence, where again the single terms are not divisible by $\mathfrak{P}^{e\delta}$. In either case therefore a non-identical congruence of the form (27) has been created and this under the assumption that $\nu<ef$.

ART. **254.** It has been proved that in any realm the discriminant of a fundamental system of basal elements is (mod. p), and in so far as the divisibility by p is considered, equivalent to the discriminant (fundamental invariant = *Grundzahl*) of the realm. Hence the discriminant of the basal elements (23) is divisible by the same power of p as is the discriminant of the realm $\mathfrak{R}(\pi_{11}, \rho)$.

It has been proved also that if $\mathfrak{K}$ is a realm of degree N, and if $\mathfrak{k}$ is a sub-realm of degree n, and if Θ is a quantity that determines $\mathfrak{K}$, so that $\mathfrak{K}=\mathfrak{R}(\Theta)$, and if further

$$\Theta^r+\alpha_1\Theta^{r-1}+\cdots+\alpha_r=0,$$

is the equation of lowest degree that Θ satisfies, where the α's are quantities in $\mathfrak{k}$, then r is the relative degree of $\mathfrak{K}$ and $N=rn$. If $\Omega_1, \Omega_2, \cdots, \Omega_N$ are a system of basal elements of $\mathfrak{K}$, the square of the greatest common divisor of all the determinants of r-order in the matrix

$$\begin{vmatrix} \Omega_1, & \Omega_2, & \cdots, & \Omega_N \\ \Omega_1', & \Omega_2', & \cdots, & \Omega_N' \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ \Omega_1^{(r-1)}, & \Omega_2^{(r-1)}, & \cdots, & \Omega_N^{(r-1)} \end{vmatrix} \bullet$$

is the relative discriminant $\mathfrak{D}_\mathfrak{r}$ of $\mathfrak{R}$ with respect to $\mathfrak{r}$. (See Art. 184.) This relative discriminant is clearly an ideal. If D is the discriminant of $\mathfrak{R}$ and if d is the discriminant of $\mathfrak{r}$, then is

$$D = d^r \cdot n(\mathfrak{D}_\mathfrak{r})$$

(Art. 186), where n denotes the norm taken in $\mathfrak{r}$. Observe that (Art. 229)

$$N(\mathfrak{P}) = p^f,$$

where N is the norm taken in $\mathfrak{R}$. Accordingly, it is seen that the discriminant of $\Re(\pi_{11}, \rho_1)$ is equal to the product of the eth power of the discriminant of the equation (20) namely $P(x) = 0$, which ρ_1 satisfies, multiplied by the norm of the relative discriminant of $\psi_1(x) = 0$, which is satisfied by π_{11}.

As the eth power of the first discriminant is not divisible (Art. 94) by p, since $P(x)$ is irreducible (mod. p), it is seen that the relative discriminant of $\psi_1(x)$ is, so far as divisibility by p is concerned, equivalent to the discriminant of $\Re(\pi_{11}, \rho_1)$.

The relative discriminant in question is

$$\Pi(\pi_{1\alpha} - \pi_{1\beta}) \qquad (\alpha \gtrless \beta = 1, 2, \cdots, e);$$

while the norm of this expression is

$$\Pi(\Psi'_k(\pi_{kh})), \qquad \begin{pmatrix} k = 1, 2, \cdots, f \\ h = 1, 2, \cdots, e \end{pmatrix},$$

and this is with respect to the image realm $\Re(\pi_{11}, \rho_1)$ the norm of $\Psi'_1(\pi_{11})$.

Next observe that the complex of those numbers of the image realm $\Re(\pi_{11}, \rho_1)$, which correspond to the numbers of an ideal in $\Re(\omega)$, constitute an ideal in $\Re(\pi_{11}, \rho_1)$ and vice versa. For if α is a number of an ideal in $\Re(\omega)$ and if α_1 is the corresponding number in the image realm, and if ζ_1 is an integer of $\Re(\pi_{11}, \rho_1)$ that corresponds to ζ in $\Re(\omega)$, then, as $\zeta\alpha$ is a number of the ideal in $\Re(\omega)$, it

follows that $\zeta_1\alpha_1$ is a number of the complex in $\Re(\pi_{11}, \rho_1)$, and this complex characterizes an ideal. It is clear that two corresponding ideals are simultaneously prime ideals and in particular they are simultaneously prime divisors of p; and it is also clear that when one ideal is a divisor of π, the other is a divisor of π_{11} and vice versa. Accordingly, it is seen that in the image realm there exists a single prime ideal factor $\bar{\mathfrak{p}}$ of p which is a divisor of π_{11} and exactly to the first degree.

We may say, after Kronecker, $\bar{\mathfrak{p}}$ is equivalent to $pz+\pi_{11}n$ where z and n are rational integers; and we may write

$$\bar{\mathfrak{p}} \sim pz+\pi_{11}n.$$

From equation (30), which is satisfied by π_{11}, it is seen that p is equivalent to $\bar{\mathfrak{p}}^e$ or $\bar{\mathfrak{p}}$ is equivalent to $p^{\frac{1}{e}}$; and consequently with respect to the image realm, which is of degree ef, the norm of $\bar{\mathfrak{p}}$ is equivalent to p^f, and that is

$$N(\bar{\mathfrak{p}}) \sim p^f.$$

Further note in the expression

$$\Psi'(\pi) = e\pi^{e-1}+pC_{e-1}(e-1)\pi^{e-2}+\cdots+pC_1,$$

that each term to the right is, with respect to $\mathfrak{p}$, of different order, the order of the entire expression being the order of its lowest term. Similarly the order of $\Psi_1'(\pi_{11})$ is, with respect to $\bar{\mathfrak{p}}$, the order of its lowest term; and if it is denoted by $\mathfrak{p}^{v-1}$, then the entire expression $\Psi_1'(\pi_{11})$ is equivalent to the fractional power $p^{\frac{v-1}{e}}$. The same is true of the conjugate factors of the product (36). Accordingly, this product is equivalent to

$$(p^{\frac{v-1}{e}})^{ef} = p^{(v-1)f}.$$

Having regard to the notation of Art. 252, the number v

may be called the *branch-number*, while the discriminant of the image realm may be called the *branch-discriminant.*

In the *regular* case

$$v=e; \tag{37}$$

for in this case

$$\Psi(x)=x^e+pB_0, \tag{38}$$

so that

$$\psi'(\pi_{11})=e\pi_{11}^{e-1},$$

which expression, since e is not divisible by p, is of the order $e-1$, and e is the branch-number. In the *singular* case, however, $\Psi(x)$ is of the more general form (17), and if we put $e=pC_e$, it is seen that

$$\Psi_1'(\pi_{11})=pC_e\pi_{11}^{e-1}+pC_{e-1}(e-1)\pi_{11}^{e-2}+\cdots+pC_i i\pi_{11}^{i-1}+\cdots+pC_1.$$

If then $pC_i i$ is that coefficient, which *firstly* contains the lowest power p^{ϵ_i} of p and in which *secondly* the exponent i is the smallest, then is $\Psi_1'(\pi_{11})$ of the order $e\epsilon_i+i-1$, that being the order of the term $pC_i i\pi_{11}^{i-1}$, and consequently the branch number is here

$$v=e\epsilon_i+i. \tag{37a}$$

The general result may be expressed as follows: *If* $\mathfrak{p}$ *is a prime ideal factor of the fth degree occurring to the eth power as a factor of* p *in the realm* $\Re(\omega)$, *and if the image realm is* $\Re(\pi_{11}, \rho_1)$, *then the discriminant of the latter realm is exactly divisible by* $p^{(v-1)f}$, *where* v *is the branch-number determined through the formulas (37) and (37a).*

The branch-number has its least value in the regular case, where $v=e$; for in the singular case, even when $\psi(x)$ has the simple form (38), it is seen that v is greater than e, since both ϵ_i and i are at least equal to unity. And in the singular case clearly v reaches its greatest value if $e\pi_{11}^{e-1}$ is the term of lowest order in $\Psi_1'(\pi_{11})$, and in this case $v=(\epsilon+1)e$, if e is exactly divisible by p^{ϵ}.

Dedekind expressed this result as a conjecture at the end of his paper "Ueber die Discriminanten endlicher Körper." (*Gött. Abh.*, Vol. 29, 1882.)

ART. **255.** We may denote the integer ω and its conjugates by

$$\omega_1, \omega_2, \cdots, \omega_n \tag{39}$$

and denote by

$$\Re(\omega_1), \Re(\omega_2), \cdots, \Re(\omega_n) \tag{40}$$

the realm $\Re(\omega)$ and its conjugate realms. Let $\mathfrak{K}$ be a Galois realm that is constituted of the realms (40) and let $\mathfrak{P}$ be an arbitrary prime ideal factor of p in $\mathfrak{K}$. Then among the prime ideal factors into which p is factored in each of the conjugate realms (40) there are in each realm prime ideal factors $\mathfrak{p}^{(1)}, \mathfrak{p}^{(2)}, \cdots, \mathfrak{p}^{(n)}$, each of which is divisible by $\mathfrak{P}$. With respect to each of these prime ideals, let the results of Art. 251 be repeated, so that to the two numbers ρ, π of Art. 251 there correspond numbers $\rho^{(i)}$, $\pi^{(i)}$ $(i=1, 2, \cdots, n)$, which satisfy congruences analogous to (15) and (16), namely

$$P^{(i)}(x) \equiv 0, \qquad \Psi^{(i)}(x) \equiv 0 \pmod{\mathfrak{p}^{(i)m}} \quad (i=1, 2, \cdots, n).$$

From the roots of the equations that are analogous to (20) and (21), namely

$$P^{(i)}(x) = 0, \qquad \Psi_t^{(i)}(x) = 0, \tag{41}$$

the realm $\Re(\pi_{11}^{(i)}, \rho_1^{(i)})$ with its conjugates is determined.

Suppose that this has been done for each of the prime ideal factors $\mathfrak{P}$ of p in $\mathfrak{K}$, and let $\mathfrak{K}_{\bar{\sigma}}$ be a Galois realm which includes the Galois realm $\mathfrak{K}_\sigma$ of Art. 253 and besides all the realms $\Re(\pi_{11}^{(i)}, \rho_1^{(i)})$ with their conjugates. Let $\mathfrak{P}$ be any prime ideal factor of p in $\mathfrak{K}_{\bar{\sigma}}$. It is clear that the results of the preceding article are true with respect to $\mathfrak{P}$ for each of the conjugate realms (40). Thus for every realm $\Re(\omega_i)$ there may be determined another

definite realm $\Re(\pi_{11}^{(i)}, \rho^{(i)})$ upon which $\Re(\omega_i)$ may be imaged (mod. $\mathfrak{P}^m$) and vice versa; and this is effected by determining a quantity $\omega_i^{(0)}$ of $\Re(\pi_{11}^{(i)}, \rho^{(i)})$ of the form

$$\omega_i^{(0)} = A_{r_i}^{(i)}\pi_{11}^{(i)r_i} + A_{r_i+1}^{(i)}\pi_{11}^{(i)r_i+1} + \cdots \quad (i=1, 2, \cdots, n), \tag{42}$$

for which

$$\omega_i \equiv \omega_i^{(0)} \text{ (mod. } \mathfrak{P}^m). \tag{43}$$

In this manner [1] we have for the n conjugate realms

$$\Re(\omega_1), \Re(\omega_2), \cdots, \Re(\omega_n)$$

a like number of image realms

$$\Re(\pi_{11}^{(1)}, \rho_1^{(1)}), \Re(\pi_{11}^{(2)}, \rho_1^{(2)}), \cdots, \Re(\pi_{11}^{(n)}, \rho_1^{(n)}) \text{ (mod. } \mathfrak{P}^m). \tag{44}$$

If as above

$$F(x) = (x-\omega_1)(x-\omega_2)\cdots(x-\omega_n) = 0 \tag{45}$$

is the equation with rational integral coefficients that is satisfied by the quantities (39), then, due to (43), it is seen that

$$F(x) \equiv (x-\omega_1^{(0)})(x-\omega_2^{(0)})\cdots(x-\omega_n^{(0)}) \text{ (mod. } \mathfrak{P}^m);$$

and that is, each of the numbers (42) is a root of the congruence

$$F(x) \equiv 0 \text{ (mod. } \mathfrak{P}^m). \tag{46}$$

Further any root of (46) must be congruent to one of the numbers (42) with respect to an arbitrarily high power of $\mathfrak{P}$. Moreover, these roots are incongruent (mod. $\mathfrak{P}^m$); otherwise the discriminant would be divisible by an arbitrarily high power of p, since the discriminant is a rational integer. But this discriminant is *not* zero due to the fact that the equation $F(x)=0$ is irreducible.

The n quantities are also characterized as the roots of the congruence

$$F(x) \equiv 0, \tag{47}$$

taken with respect to an arbitrarily high power of p as

[1] Hensel, *Math. Ann.*, 55, p. 311.

modulus. For develop the expression $F(\omega_i^{(0)})$ with respect to the powers of $\rho_1^{(1)}$ and $\pi_{11}^{(1)}$. Then observe that the congruence

$$F(\omega_i^{(0)}) \equiv 0 \text{ (mod. } \mathfrak{P}^m),$$

when reduced through equations (41) of degrees respectively f_i and e_i in $\rho_1^{(1)}$ and $\pi_{11}^{(1)}$, has the form

$$\sum_{g=0}^{f^{(i)}-1} \sum_{h=0}^{e^{(i)}-1} a_{gh} \rho_1^{(1)g} \pi_{11}^{(1)h} \equiv 0 \text{ (mod. } \mathfrak{P}^m).$$

It was proved in Art. 253 that this expression can only exist identically, and that is, each of the terms $a_{gh}\rho_1^{(1)g}\pi_{11}^{(1)h}$ must of itself be divisible by $\mathfrak{P}^m$. Hence for a sufficiently large value of m each of the coefficients a_{gh} is divisible by an arbitrarily large value of $\mathfrak{P}$ and therefore by a correspondingly large value of p; and that is the congruence (47), with respect to this arbitrarily large value of p as a modulus, is satisfied by the number $\omega_i^{(0)}$.

If $\omega_i^{(0)}$ satisfies the congruence $F(x) \equiv 0$ (mod. $\mathfrak{P}^m$), the same is true of all the $e^{(i)}f^{(i)}$ numbers conjugate to $\omega_i^{(0)}$ taken in the image realm $\Re(\pi_{11}^{(1)}, \rho_1^{(1)})$ of degree $e^{(i)}f^{(i)}$, to which $\omega_i^{(0)}$ belongs. Accordingly, these $e^{(i)}f^{(i)}$ numbers are all roots of the congruence (46) with respect to the modulus $\mathfrak{P}^m$. Further these roots are different; for were any two of them congruent (mod. $\mathfrak{P}^m$), then the discriminant of these numbers, that is the discriminant of the irreducible equation of degree $e^{(i)}f^{(i)}$, which (Art. 253) the number $\omega_i^{(0)}$ of this degree satisfies, would be divisible by $\mathfrak{P}^m$; or since this discriminant is a rational integer, it would consequently be divisible by an arbitrarily high power of p. And that is, the discriminant would be zero, which is not true.

From this it is seen that the n numbers (42) (mod. $\mathfrak{P}^m$) may be distributed into sets of $e^{(i)}f^{(i)}$ numbers which are congruent to numbers in the image realms, these numbers

being conjugate among themselves. This is true for every value of the index i. Observe that

$$n = \sum e^{(i)} f^{(i)}.$$

Accordingly we have the following theorem: *The n image realms (44) may be distributed into a number of systems of realms, in each of which there is a number of realms less than n that are conjugates amongst themselves.*

For example, if the prime integer p in the realm $\Re(\omega)$ is factorable as a product of three prime ideals, say $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$, of degrees f_1, f_2, f_3, so that

$$p = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \mathfrak{p}_3^{e_3},$$

then there are three systems of respectively

$$\nu_1 = e_1 f_1, \qquad \nu_2 = e_2 f_2, \qquad \nu_3 = e_3 f_3 \quad (n = \nu_1 + \nu_2 + \nu_3)$$

realms that are conjugate among themselves, say

$$\Re(\gamma_1), \Re(\gamma_2), \cdots, \Re(\gamma_{\nu_1}); \ \Re(\delta_1), \cdots, \Re(\delta_{\nu_2}); \ \Re(\epsilon_1), \cdots, \Re(\epsilon_{\nu_3}),$$

upon which the n realms $\Re(\omega_1), \Re(\omega_2), \cdots, \Re(\omega_n)$ are imaged (mod. $\mathfrak{P}^m$) uniquely.

It may be proved without difficulty that the above are realms of the least degree, upon which the realms $\Re(\omega_i)$ $(i = 1, 2, \cdots, n)$ may be imaged (mod. $\mathfrak{P}^m$) uniquely.

ART. **256.** Let ζ_1 be any integer of $\Re(\omega_1)$ and denote by $\zeta_2, \cdots, \zeta_n$ its conjugates; then is ζ_1 congruent (mod. $\mathfrak{P}^m$) to a number of the image realm $\Re(\gamma_1) = \Re(\pi'_{11}, \rho'_1)$; and there exists [see formula (14)], a congruence of the form

$$\text{(F)} \qquad \zeta_1 \equiv \sum_{g=0}^{f_1-1} \sum_{h=0}^{e_1-1} a_{gh} \rho'^{g} \pi'^{h} \ (\text{mod. } \mathfrak{P}^m);$$

or more simply, if the $\nu_1 = e_1 f_1$ numbers $\rho'^{g}_1 \pi'^{h}_{11}$ be arbitrarily, but in definite order (Hensel, *Math. Ann.*, Vol. 55,

p. 322), denoted by

$$\gamma_1^{(1)},\ \gamma_1^{(2)},\ \cdots,\ \gamma_1^{(\nu_1)}, \tag{48}$$

then ζ_1 takes the form

$$\zeta_1 \equiv a_1\gamma_1^{(1)}+a_2\gamma_1^{(2)}+\cdots+a_{\nu_1}\gamma_1^{(\nu_1)} \pmod{\mathfrak{P}^m}.$$

If $\gamma_i^{(1)}, \gamma_i^{(2)}, \cdots, \gamma_i^{(\nu_1)}$ denote the conjugates of the numbers (48) which belong to the realm $\Re(\gamma_i)(i=1, 2, \cdots, \nu_1)$, it is seen that, for the numbers ζ_i which are the conjugates of ζ_1, there exist the congruences

$$\zeta_i \equiv a_1\gamma_i^{(1)}+a_2\gamma_i^{(2)}+\cdots+a_{\nu_1}\gamma^{(\nu_1)} \pmod{\mathfrak{P}^m} \quad (i=1, 2, \cdots, \nu_1); \tag{48a}$$

and we find, using an analogous meaning of symbols $\delta_1^{(1)}, \delta_1^{(2)}, \cdots, \delta_1^{\nu_2}$; $\epsilon_1^{(1)}, \epsilon_1^{(2)}, \cdots, \epsilon_1^{(\nu_3)}$, the further congruences

$$\zeta_{\nu_1+h} \equiv b_1\delta_h^{(1)}+b_2\delta_h^{(2)}+\cdots+b_{\nu_2}\delta_h^{(\nu_2)} \quad (h=1, 2, \cdots, \nu_2); \tag{48b}$$

and

$$\zeta_{\nu_1+\nu_2+k} \equiv c_1\epsilon_k^{(1)}+c_2\epsilon_k^{(2)}+\cdots+c_{\nu_3}\epsilon_k^{(\nu_3)} \quad (k=1, 2, \cdots, \nu_3). \tag{48c}$$

Next let

$$\zeta_1^{(1)},\ \zeta_1^{(2)},\ \cdots,\ \zeta_1^{(n)} \tag{49}$$

denote an independent system of n integers of the realm $\Re(\omega_1)$. Construct with these integers and their conjugates the determinant

$$\begin{vmatrix} \zeta_1^{(1)}, & \zeta_1^{(2)}, & \cdots, & \zeta_1^{(n)} \\ \zeta_2^{(1)}, & \zeta_2^{(2)}, & \cdots, & \zeta_2^{(n)} \\ \cdots\cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots \\ \zeta_n^{(1)}, & \zeta_n^{(2)}, & \cdots, & \zeta_n^{(n)} \end{vmatrix}. \tag{50}$$

For each of the numbers (49) write the corresponding congruences (48a, b, c), so that in each column of the determinant the first ν_1 elements (mod. $\mathfrak{P}^m$) are replaced by linear functions of the numbers $\gamma_1^{(1)}, \gamma_1^{(2)}, \cdots, \gamma_1^{(\nu_1)}$ and their conjugates; the ν_2 following numbers in these columns by linear functions of $\delta_1^{(1)}, \delta_1^{(2)}, \cdots, \delta_1^{(\nu_2)}$ and their conjugates, etc.

A consideration of the highest powers of $\mathfrak{P}$, which are common to all the elements of a column, permits [1] *through a series of simple transformations, the system* (*49*) *to be replaced by another system, say,*

$$\xi_1^{(1)}, \xi_1^{(2)}, \cdots, \xi_1^{(n)} \tag{51}$$

of n independent numbers, which have the property that the determinant corresponding to the one above is (*mod.* $\mathfrak{P}^m$) *congruent to the following determinant:*

$$\left|\begin{array}{cccccccc}
\gamma_1^{(1)}, & \cdots, & \gamma_1^{(\nu_1)}, & 0, & \cdots, & 0, & 0, & \cdots, 0 \\
\cdots\cdots & & & & & & & \\
\gamma_{\nu_1}^{(1)}, & \cdots, & \gamma_{\nu_1}^{(\nu_1)}, & 0, & \cdots, & 0, & 0, & \cdots, 0 \\
0, & \cdots, & 0, & \delta_1^{(1)}, & \cdots, & \delta_1^{(\nu_2)}, & 0, & \cdots, 0 \\
\cdots\cdots & & & & & & & \\
0, & \cdots, & 0, & \delta_{\nu_2}^{(1)}, & \cdots, & \delta_{\nu_2}^{(\nu_2)}, & 0, & \cdots, 0 \\
0, & \cdots, & 0, & 0, & \cdots, & 0, & \epsilon_1^{(1)}, & \cdots, \epsilon_1^{(\nu_3)} \\
\cdots\cdots & & & & & & & \\
0, & \cdots, & 0, & 0, & \cdots, & 0, & \epsilon_{\nu_3}^{(1)}, & \cdots, \epsilon_{\nu_3}^{(\nu_3)}
\end{array}\right| . \tag{52}$$

It is clear that the system (51) must form a fundamental system (mod. p). (See Hensel, *op. cit.*) For were there to exist a congruence

$$u_1\xi_1^{(1)}+u_2\xi_1^{(2)}+\cdots+u_n\xi_1^{(n)}\equiv 0 \pmod{p}$$

with integral coefficients, then would this expression, as also the conjugate expressions, be divisible by the same power of the Galois prime ideal $\mathfrak{P}$, through which p is divisible; and consequently were $\mathfrak{P}^\mu$ this power, it would follow from the congruence of the matrix of that system with the determinant (52) with respect to an arbitrarily high power of $\mathfrak{P}$, that

$$\left.\begin{array}{l}
u_1\gamma_i^{(1)}+u_2\gamma_i^{(2)}+\cdots+u_{\nu_1}\gamma_i^{(\nu_1)}\equiv 0 \\
\qquad\qquad (i=1, 2, \cdots, \nu_1) \\
u_{\nu_1+1}\delta_h^{(1)}+u_{\nu_1+2}\delta_h^{(2)}+\cdots+u_{\nu_1+\nu_2}\delta_h^{(\nu_2)}\equiv 0 \\
\qquad\qquad (h=1, 2, \cdots, \nu_2) \\
u_{\nu_1+\nu_2+1}\epsilon_k^{(1)}+\cdots+u_{\nu_1+\nu_2+\nu_3}\epsilon_k^{(\nu_3)}\equiv 0 \\
\qquad\qquad (k=1, 2, \cdots, \nu_3)
\end{array}\right\} \pmod{\mathfrak{P}^\mu}.$$

[1] See Hensel, *Math. Ann.*, 55, p. 326, §§7 and 8.

It is seen from formula (F) at the beginning of this article that such congruences can only exist, if all the u's are divisible by p.

Returning to the discriminant of the system (51), it is clear that in so far as the question is regarding the divisibility by p, this discriminant is equivalent to the discriminant D of the realm $\Re(\omega_1)$. On the other hand with respect to the modulus $\mathfrak{P}^m$, the discriminant of (51) is congruent to the square of the determinant (52), and that is to the product

$$\Gamma^2 \cdot \Delta^2 \cdot E^2, \tag{53}$$

in which Γ^2, Δ^2, E^2 are equivalent to the discriminants of the systems $\gamma_k^{(l)}$, $\delta_k^{(l)}$, $\epsilon_k^{(l)}$, and that is to the different branch-discriminants with respect to p.

Observe that $\mathfrak{P}$ is an arbitrary prime ideal factor of p in $\Re_{\bar{\varrho}}$, and therefore $\mathfrak{P}$ as a factor of the discriminant D must appear exactly to the same degree, as it enters in the product (53).

With this we have the following elegant theorem of Hensel's:

Every prime ideal factor $\mathfrak{P}$ of p in $\Re_{\bar{\varrho}}$ and consequently the prime integer p itself is contained as a factor in the discriminant D of $\Re(\omega)$ exactly so often as it appears in the product of the branch-discriminants for this realm with respect to the integer p.

Accordingly, the theorems found at the end of Art. 254 offer a means of determining the exact expression for the power of p, through which D is divisible. For if we again write, for example

$$p = \mathfrak{P}_1^{e_1} \mathfrak{P}_2^{e_2} \mathfrak{P}_3^{e_3},$$

where $\mathfrak{P}_1$, $\mathfrak{P}_2$, $\mathfrak{P}_3$ are different prime ideal factors of p in $\Re(\omega)$ of degrees f_1, f_2, f_3 respectively, and if v_1, v_2, v_3 are the corresponding branch-numbers determined as in Art.

254, then is D exactly divisible by p^d, where

$$d=(v_1-1)f_1+(v_2-1)f_2+(v_3-1)f_3. \tag{54}$$

For the regular case where the e's are not divisible by p,

$$d=(e_1-1)f_1+(e_2-1)f_2+(e_3-1)f_3.$$

For the singular case where at least one of the e's is divisible by p, the first value of d is greater than the value just written. We thus have a confirmation of the theorem of Arts. 75, 77, 92, 249 which theorem offered a minimum value of the power of p which enters as a factor of D, while the theorem of Hensel offers, through formula (54) a means of determining *exactly* and in what manner the determinant of a realm, that is, the fundamental invariant (*Grundzahl*), may be decomposed into its prime ideal factors.

For further developments of this theory see Hensel, *Theorie der algebraischen Zahlen*, Chapt. XII. For numerous other references see paper by Ö. Ore, *Math. Ann.*, Vol. 96, p. 312.

INDEX

(*The numerals refer to pages*)

Abelian equation. (*See* equation.)
Affect, the, 461.
Arrangements, 479.
Associate number, 12, 299, 301, 349, 534, 629.

Basal invariant. (*See* invariant.)
Basis complementary, 211, 217.
  form. (*See* fundamental form.)
  of all integers of a realm, 8, 182, 200, 223, 248, 267, 293, 610, 637.
  of a modul, 3, 212.
  of an ideal, 49, 51, 110, 322, 336, 364, 370, 634.
  of relative realm, 392 ff.
Belongs to. (*See* permit.)
  belonging to, a function.
  to a group, 473, 491 ff.
Boundary in n dimensions, 272 ff., 301.
Branch position, 630 ff.

Cells, or cuboids, 272 ff., 299 ff.
Classes, composition of 368.
  class-realms, 420 ff.
  half-equivalent, 363.
  number, 322.
  number of, 100 ff., 104 ff., 107, 151, 293 ff., 313 ff., 320, 322, 345, 346 ff., 353.
  odd number of, 408, 413, 419, 425.
  of equivalent forms. (*See* forms.)
  of ideals, 96, 290, 293 ff., 321, 366 ff.
  principal, 97, 98, 303, 314, 323, 324 ff., 327, 344, 362, 394, 422.
  product of, 98.
  reciprocal, 97, 100, 313, 351, 362.
  system of fundamental, 323.
Congruence, functional, 115, 171.
  number, 115, 171.
  of an integer and a form, 117 ff.
  of the mth degree, 73.
  satisfied by fundamental form, 136.
  two simultaneously satisfied, 65, 198, 344.
  with respect to an ideal, 37, 64.
Conjugate divisors. (*See* conjugate groups.)
  forms. (*See* forms.)
  functions or quantities, 493, 495.
Content of a form, 124 ff., 138, 148, 387.
Cycles, 474 ff., 521 ff.
Cyclic equation. (*See* equation.)
Cyclic group. (*See* permutation.)

Development numbers, 626, 632.
Different, the, 141, 209, 213, 330, 387, 388, 571.
  of inertia realm, 610.
  relative, 381 ff., 387, 388, 392, 398, 402, 611, 614.
Dirichlet Series, 304 ff., 315 ff.
  zeta-function, 317.
Discriminant. (*See also* basal invariant.)
  branch-, 640, 647 ff.
  divisors of, 59, 60, 63, 139, 141, 162 ff., 166, 168, 176, 180, 194 ff., 216, 330, 350, 537, 560.
  negative, 222.
  of fundamental equation, 140, 166.
  partial, 536, 538 ff., 560.
  relative, 381 ff., 385, 398, 402, 407, 408 ff., 409, 412, 428, 533 ff., 638.

Divisibility by a complex of numbers, 2.
and equality for moduls and ideals, 16.
and linear forms, 2, 4, 5.
by an ideal, 5, 6, 297, 350.
by a number of ideals, 40.
by a prime integer, 1.
by prime ideals, 52, 146.
extended notion of, 2.
of a number by ideals, 41, 42, 139, 297.
Divisor of algebraic integers, 205.
irregular, of discriminant, 162 ff., 168, 176 ff., 191.
normal, 555.
of a group or sub-group, 455, 488, 489, 492 ff., invariantive, 500, 539, 543, 573 ff., 608.
of a realm. (*See* realm.)
realms which belong to a prime ideal, 548 ff.
regular, of discriminant, 194 ff.
singular, of discriminant, 216, 627, 631, 648.
Domain of points, 271 ff., 275.

Elements, Hilbert's, 140, 218, 387, 572, 610.
Equation, Abelian, 515, 517 ff., 519, 564, 606, 607.
cyclic, 523 ff.
Galois or normal, 445 ff., 569, 595.
imprimitive, 467.
linear, 235 ff., 239.
normal, 516.
relative Galois, 602.
Equivalent ideals. (*See* equivalent.)
in the narrower sense, 430 ff.
Exponents of a number, 296 ff.
of a unit, 239, 243, 340.

Factorization. (*See* divisibility.)
unique, 1, 53 ff., 147, 164.
Fermat's theorem, 72, 133, 177, 541, 554.
Form, composite (factorable), 354 ff., 371 ff., 375.
composite unit, 364 ff., 377.
conjugate, 123, 145.
equivalent, 51, 123, 128, 355.
fundamental. (*See* fundamental.)
integral homogeneous, 49.
Kronecker, 123 ff.
linear, 4, 5, 177 ff., 225 ff., 235, 247, 255, 257, 276, 284 ff., 289, 299, 349, 354, 361.
prime, 124.
primitive, 51, 127, 357.
unit, 124 ff., 357, 360 ff., 370 ff., 384.
Functions, conjugate, 493.
Fundamental classes, 323 ff.
equation, 130, 138, 140, 165 ff., 177, 184, 187, 218, 631.
form, 130 ff., 166 ff., 177 ff., 184, 187, 261, 330, 331, 382, 537, 556.
ideal. (*See* ideal.)
theorem. (*See* theorem.)

Galois. (*See* theory; *see also* group.)
equation. (*See* equation.)
Gaussian theorem, the. (*See* theorem.)
Geometry of Numbers, 271 ff.
Greatest Common Divisor. (*See also* divisibility.)
existence proof, 154.
of groups, 499.
of ideals, 8, 11, 203.
of the differents, 213.
of two algebraic numbers, 109.
Group, alternating, 482 ff.
branch, 551, 555, 597 ff., 600, 612.
commutative or Abelian, 455, 518 ff., 539.
conjugate, 494, 502.
cyclic, 565, 602.
degree of, 451, 488, 490, 508, 544, 552.
divisors of. (*See* divisors.)
finite, 451.
Galois, defined, 458.
Galois or normal, 455 ff., 520, 573.
G. C. D., or intersection of, 499.

identical, 482.
index of. (*See* index.)
inertia, 551, 555, 574, 578.
one-stroked branch-, 603.
permutation, 452 ff., 455 ff., 469 ff.
primitive and imprimitive, 463 ff., 484, 508 ff., 514, 522.
reduction of, 504.
relative cyclic, 609.
separation, 551, 574.
simple, 501.
substitution, 451 ff., 563.
sub-. (*See* divisor.)
symmetric, 473, 484, 486.
transitive and intransitive, 462 ff., 485, 513 ff.
two-stroked, 607.

Height of algebraic integer, 77, 82, 85, 86, 87.
Height unity, 80, 82.
Henselian realms, 191 ff.

Ideals and moduls, 2, 8, 16, 17, 18.
ambiguous, 397, 402, 420.
as G. C. D. of two principal ideals, 43, 120, 157.
associated with number, 160.
as the content of a form. (*See* content.)
characteristic of, 6.
classes of, 96, 105, 293 ff., 313 ff.
complementary, 57.
conjugate.
definition of, 5, 6, 7, 130, 335.
degree of prime, 58, 82, 110, 111, 112, 137, 177, 180, 196, 319, 531, 540, 550, 560.
equality of, 158 ff.
equivalent, 96, 151, 343, 352.
fractional, 35.
fundamental (or basal), 56, 141, 194 ff., 213, 216, 217, 330, 536, 558.
greatest common divisor of, 8, 9, 17, 48, 337, 339.
infinite number of first degree, 321.

Ideal, integral, 22.
ideals of relative realm, 396.
invariantive, 566 ff., 571.
least common multiple of, 8, 9, 17, 336, 337, 339.
of the nth order, 101.
with negative exponents, 16.
norm of. (*See* norm.)
primary prime, 414, 418.
prime, 52 ff., 147 ff., 424, 530, 583.
prime (defined), 53, 146, 319.
prime, of relative realm, 400, 428.
principal, 11, 12, 23, 31, 33, 38, 43, 96, 105, 142, 152, 203, 264, 297, 334, 350, 422, 428, 568, 571.
product of, 8, 9, 337, 368.
as product of prime ideals, 54.
realm, 240.
quotient of, 8, 9, 17.
relative conjugate, 380.
relatively prime, 31, 33, 65.
relatively prime to rational integer, 39.
reciprocal, 12, 13, 17, 58, 99, 103, 313.
ring-, 336.
Ideal number. (*See* number.)
Image of algebraic integer, 299.
Image of a realm, 633 ff., 638 ff.
Imprimitivity, system of, 464 ff., 508 ff.
Incongruent integers, 203.
Incongruent residues, complete set of, 64, 86, 111, 114, 531.
Index, divisor of, 164, 170, 180, 184, 214.
of algebraic integer, 162 ff., 174, 188.
of divisor of group, 490, 503, 508, 541.
Independent, linearly. (*See* integer.)
Integers, linearly independent, 116, 199.
relative conjugate, 380.
Invariance of the inertia group, 579, 600.

Invariant, basal or fundamental (*see also* Discriminant), 19, 59, 60, 162 ff., 179, 187, 194, 202, 212, 216, 217, 241, 256, 257, 258, 290, 291, 293, 298, 328, 357, 536, 537, 572, 615, 637, 647, 648.
Irreducible function. (*See* prime function.)
Isomorphism, 457, 488, 494.

Jacobian, 275, 354.

Kummer Number. (*See* number.)

Lagrange. (*See* theorem.)
Lattice-points, 279, 298 ff., 301 ff.
Law of reciprocity, cubic, 388, 408.
  quadratic, 388, 411.
Line-distance, 280 ff.
Linear functions. (*See* forms.)

Mascheroni-Euler Constant, 317.
Metacyclic, 558.
Minkowski, theorems. (*See* theorem.)
Möbius, coefficients of, 87, 95, 179.
Modul, 359.
  and ideal, 5, 8.
  complementary, 211, 214, 217.
  composite, 137.
  definition of, 3.
  equivalent, 376.
  ring-. (*See* order-modul.)
Modular system, 189 ff., 191.
Multiple, least common of ideals, 8.

Natural irrationalities, 507.
Neighborhood of a point, 271.
Norm of algebraic unit, 219, 246.
  of a form, 124, 127, 128, 149.
  of a product, 45, 316, 318.
  of a realm, 445.
  of different, 171, 572.
  of fundamental basal ideal, 58, 218.
  of ideal, 19, 20, 197.
  of ideal expressed through φ-functions, 70.
  of integer, 229 ff., 234, 251, 322.
  of integral ideal, 31, 37, 38, 52, 290.
  partial, 536.
  relative, 381 ff., 391, 397, 528 ff., 589.
  total, 529.
Number, associated with ideal, 160.
  equivalent, 161.
  ideal (Kummer), 106, 123, 156, 165, 322.
  of classes of ideals. (*See* classes.)
  quantities, 628.
  reduced, 296 ff., 301 ff.

Order of an ideal, 8, 101.
  of a modul, 4.
  of a number, 621.
  order-modul, 3, 7, 11, 106, 110, 197, 202, 210, 218, 245, 250, 334 ff., 353, 371, 376.
  order-modul, principal, 3.

p-adic numbers, 620 ff.
  regular, 629.
Partial discriminant. (*See* discriminant.)
Period of algebraic integer, 79.
Permits a substitution, a quantity, 449, 458 ff., 462, 496, 499, 505, 509, 539.
φ-function for ideals, 65 ff.
Plane in n dimensions, 272.
Permutation, definition of, 452, 462 ff.
  composition of, 453.
  cyclic or circular, 455, 475, 555.
  degree of, 487.
  group. (*See* group.)
  of the first and second kinds, 477.
  identical, 453, 471, 475.
  inverse, 453, 471.
  order of, 475.
  period of, 487.
Primary Theorem, the. (*See* theorem.)

Prime function, 83, 85.
mod. p, 114, 116, 136 ff., 171, 173 ff., 209, 215.
primary, 88 ff.
Primitive form, 51, 127.
function, 126.
mth root of unity, 220, 244, 245.
number, 114, 117, 442 ff., 576 ff.
roots of ideals, 531, 533 ff.
Principal class. (*See* class.)
ideal. (*See* ideal.)
Product of classes, 98, 99.
of ideals, 8.
of modular systems, 172.
Prospect, a, 324, 333.

Quotient of ideals, 8.

Realm of rationality, 441.
branch, 551, 555 ff.
conjugate complex, 221, 225 ff., 256, 258, 260, 293, 529.
divisors of, sub-, 379, 386, 387, 390, 528 ff., 544 ff., 569, 595, 618.
inertia, 550 ff., 574, 593 ff.
one-stroked branch, 603 ff.
normal or Galois, 221, 332, 333, 444 ff., 561 ff.
primitive and imprimitive, 441, 443, 465, 468.
real, 221 ff., 227, 256, 258, 260, 293.
relative, 379 ff.
relative conjugate, 379.
relative cyclic, 566.
relative normal, 539 ff.
relative quadratic, 389, 390, 420, 430.
separation (reduction), 549 ff., 574, 593.
super-, or upper, 379, 387, 390, 608.
two-stroked branch, 607.
three-stroked, etc., 608.
unbranched, 420, 431.
Reciprocity. (*See* law of reciprocity.)
Reduced numbers. (*See* number.)
units. (*See* unit.)
Regulator of system of units, 243, 350.
Relative realm. (*See* realm.)
conjugate. (*See* realm.)
conjugate integers, 380.
degree of realm, 379.
different. (*See* different.)
discriminant. (*See* discriminant.)
norm. (*See* norm.)
normal realms. (*See* normal realm.)
Resolvent, the Galois, 444, 446 ff., 459, 488.
reduction of, 495.
the groups of the, 501 ff.
total and partial, 502 ff.
Retrospect, a, 328.
Ring-leader, 202 ff., 205, 208, 214, 334, 339 ff.

Singular position, 630.
Spur, of algebraic integer, 61, 197, 201, 212, 530.
Sub-groups. (*See* divisors.)
Substitution, 365.
bilinear, 370.
composition of, 450.
fundamental, 564.
group. (*See* group.)
identical, 448.
of a normal realm, 447, 449 ff., 457 ff.

Theorem of Schönemann or Eisenstein, 623.
the fundamental, 53, 147, 400.
the Galois, 441 ff.
the Gaussian (generalized), 25, 27, 121, 142 ff.
the Lagrange, 495, 497, 500, 505, 526.
the Minkowski, 255, 321 ff., 615.
the primary, 24, 28, 29, 126, 142 ff., 146, 148, 149, 153, 343.
Transformation, 366 ff.
Transpositions, 471 ff., 478.

Unique factorization. (*See* fundamental theorem.)
Unit. (*See* modul.)
algebraic, 219 ff., 530.
conjugate, 233, 234, 252, 254, 616.
existence of, 220 ff., 232, 233, 245, 246, 260, 262.
form. (*See* form.)
fundamental, 412.
fundamental system of, 242, 244, 245, 269 ff., 314, 299 ff., 304.
group, 482.
logarithms of, 233 ff., 260 ff., 265, 266 ff.
reduced, 239 ff., 243, 266 ff., 349.
system of independent, 237, 244, 255, 265, 269 ff., 616, 618.
Unity, roots of, 220, 222, 244, 269, 350.

Volume, computation of, 275 ff., 282, 285 ff., 299 ff., 301 ff.
in space of n dimensions, 273, 275 ff.

Wilson's Theorem, 76.

Zeta-function, 317 ff.